FIG.1

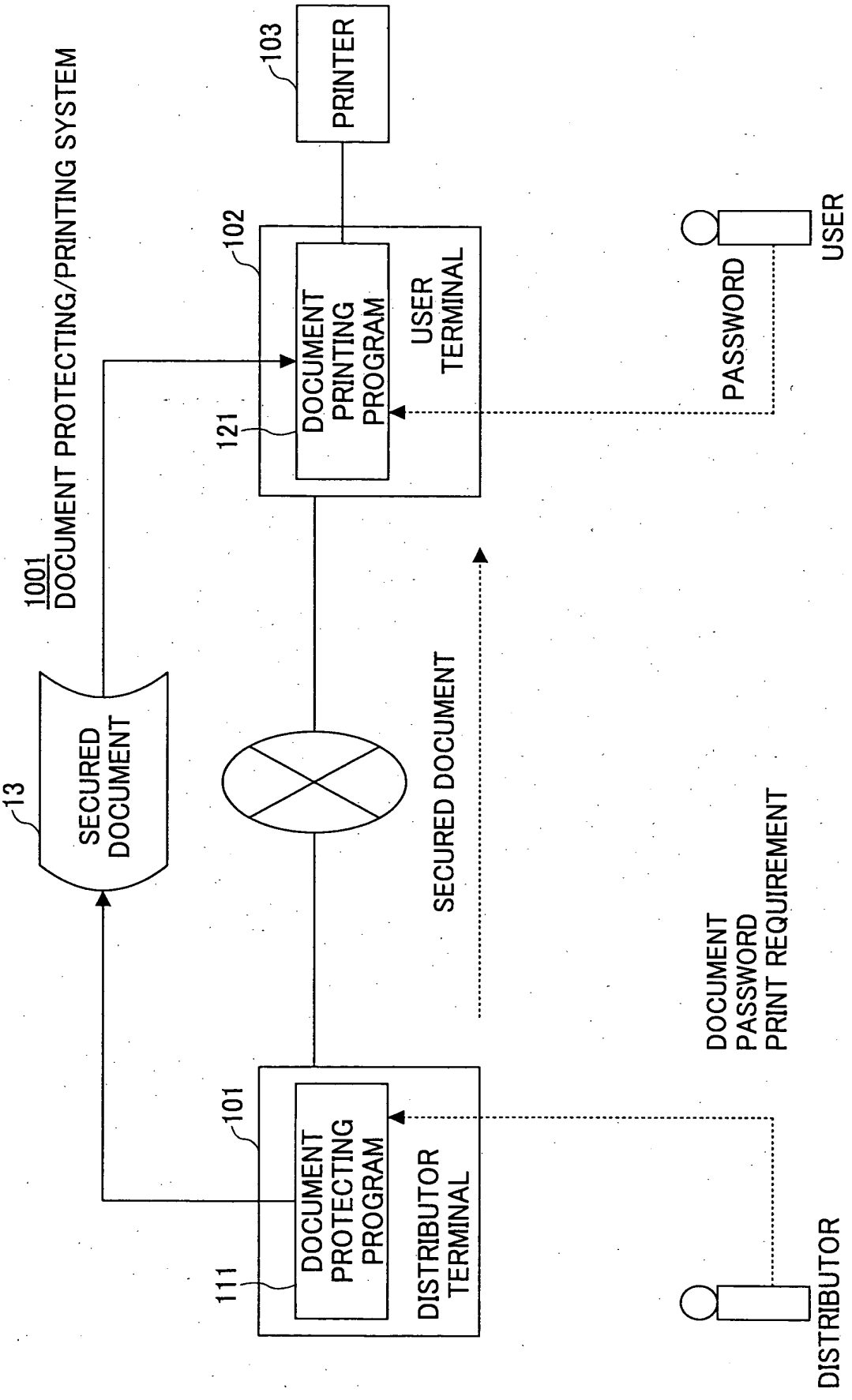
1001
DOCUMENT PROTECTING/PRINTING SYSTEM
103
PRINTER
102
USER TERMINAL
121
DOCUMENT PRINTING PROGRAM
PASSWORD
USER
13
SECURED DOCUMENT
SECURED DOCUMENT
DOCUMENT
PASSWORD
PRINT REQUIREMENT
101
DOCUMENT PROTECTING PROGRAM
111
DISTRIBUTOR TERMINAL
DISTRIBUTOR

FIG.2

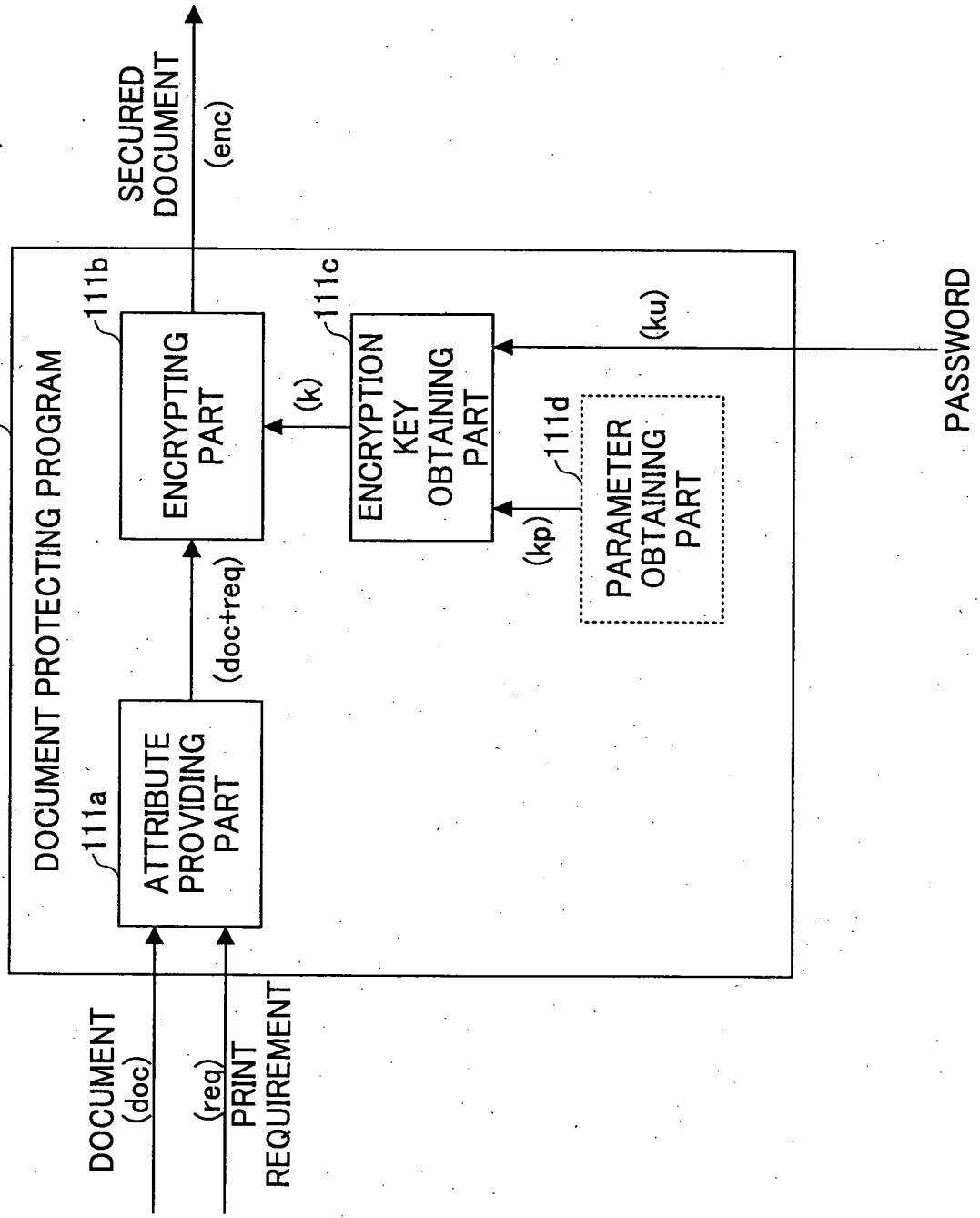
DOCUMENT (doc)
PRINT REQUIREMENT (req)
DOCUMENT PROTECTING PROGRAM
111
111a
ATTRIBUTE PROVIDING PART
(doc+req)
111b
ENCRYPTING PART
(k)
111c
ENCRYPTION KEY OBTAINING PART
(kp)
111d
PARAMETER OBTAINING PART
(ku)
PASSWORD
SECURED DOCUMENT
(enc)

FIG.3

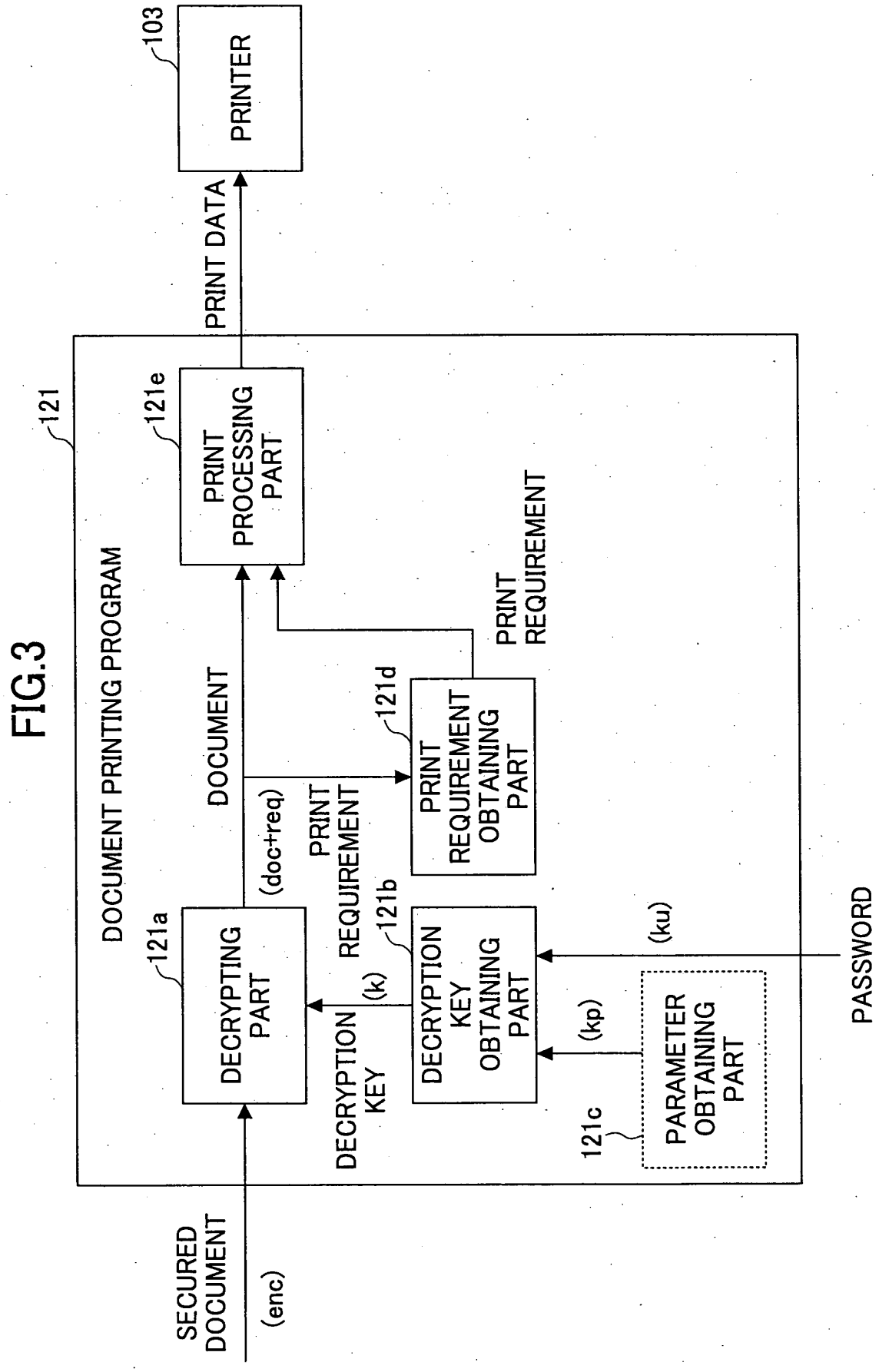
103
PRINTER
PRINT DATA
121
DOCUMENT PRINTING PROGRAM
121e
PRINT PROCESSING PART
DOCUMENT
PRINT REQUIREMENT
121d
PRINT REQUIREMENT OBTAINING PART
(doc+req)
PRINT REQUIREMENT
121a
DECRYPTING PART
121b
DECRYPTION KEY OBTAINING PART
(k)
DECRYPTION KEY
(ku)
PASSWORD
(kp)
121c
PARAMETER OBTAINING PART
SECURED DOCUMENT
(enc)

FIG.4

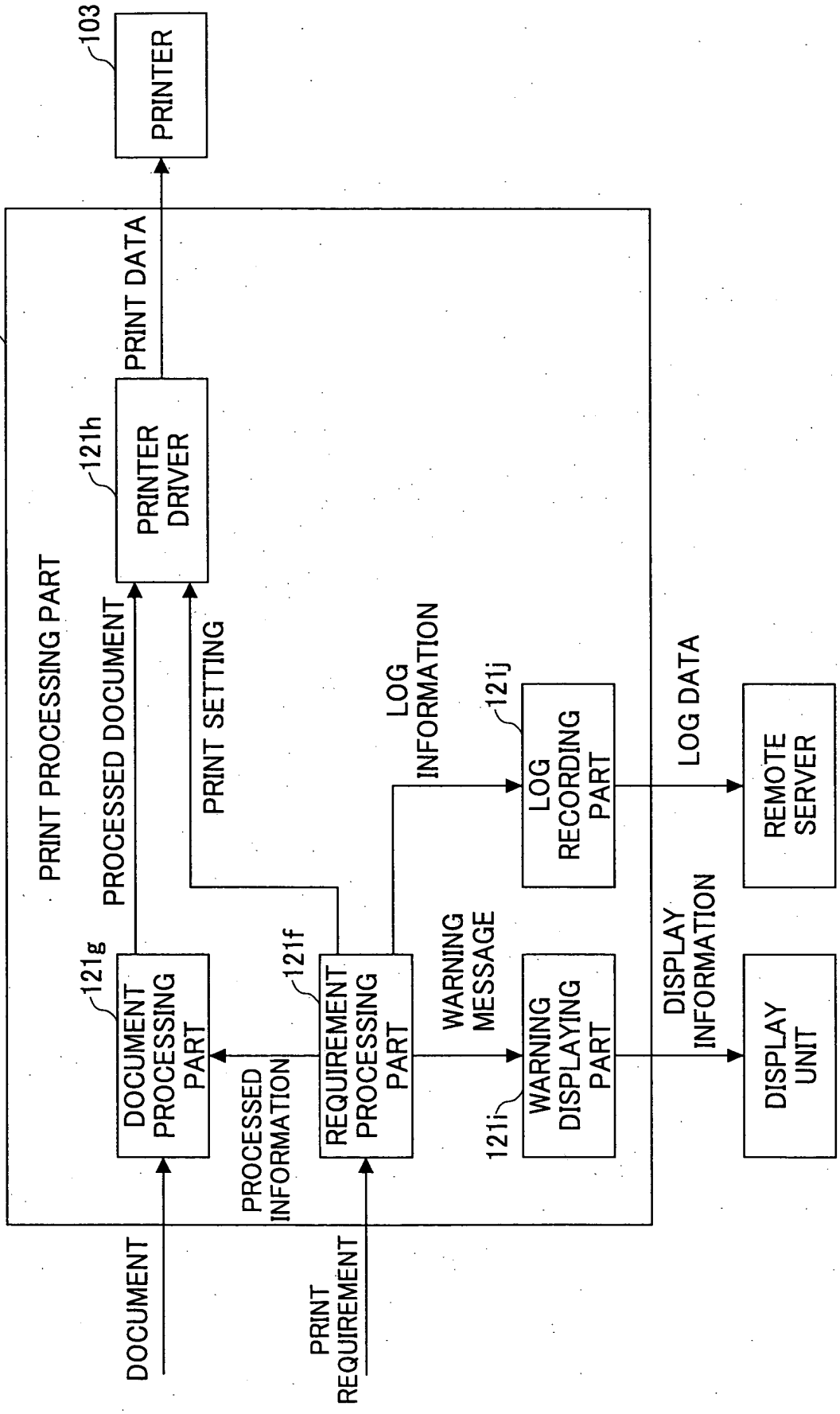
103
PRINTER
121e
PRINT PROCESSING PART
PRINT DATA
121h
PRINTER DRIVER
PROCESSED DOCUMENT
PRINT SETTING
LOG INFORMATION
121j
LOG RECORDING PART
LOG DATA
REMOTE SERVER
121g
DOCUMENT PROCESSING PART
121f
REQUIREMENT PROCESSING PART
WARNING MESSAGE
121i
WARNING DISPLAYING PART
DISPLAY INFORMATION
DISPLAY UNIT
PROCESSED INFORMATION
DOCUMENT
PRINT REQUIREMENT

FIG.5

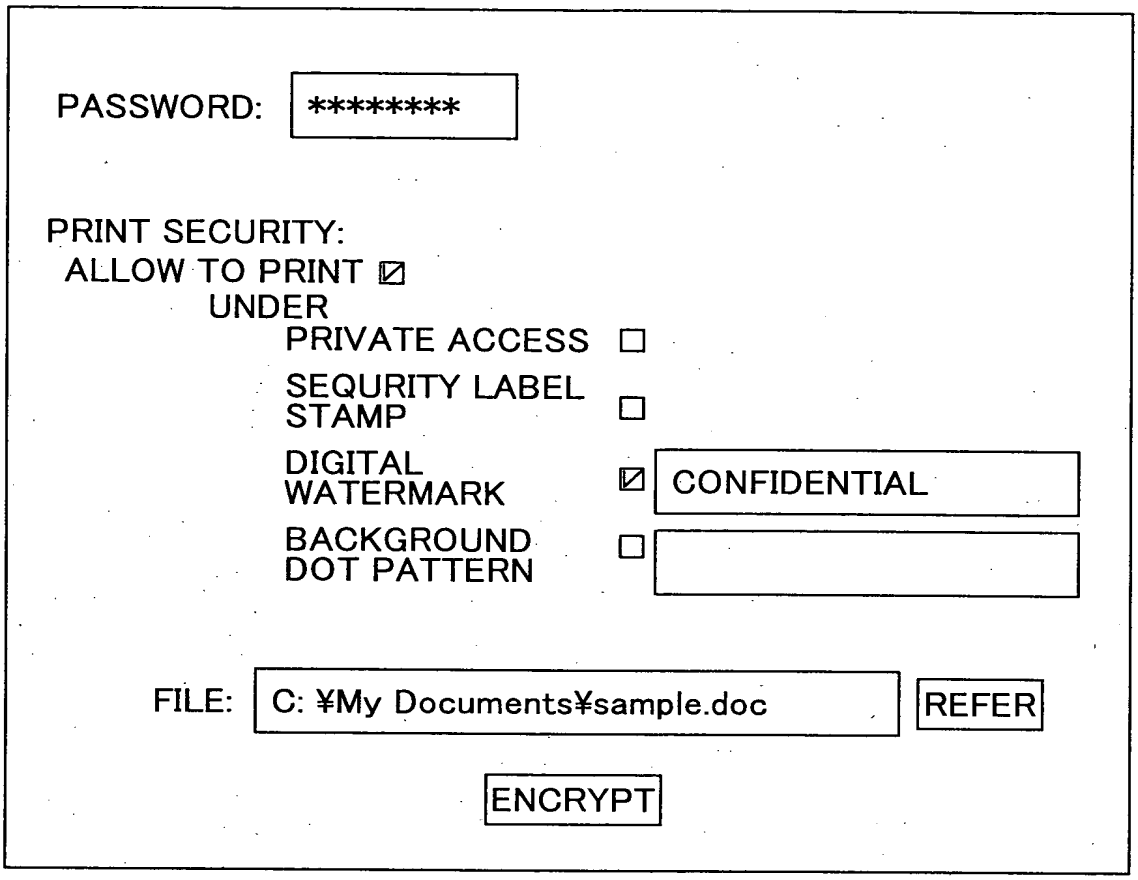
PASSWORD:
****
PRINT SECURITY:
ALLOW TO PRINT
UNDER
PRIVATE ACCESS
SEQURITY LABEL STAMP
DIGITAL WATERMARK
CONFIDENTIAL
BACKGROUND DOT PATTERN
FILE:
C: ¥My Documents¥sample.doc
REFER
ENCRYPT

FIG.6

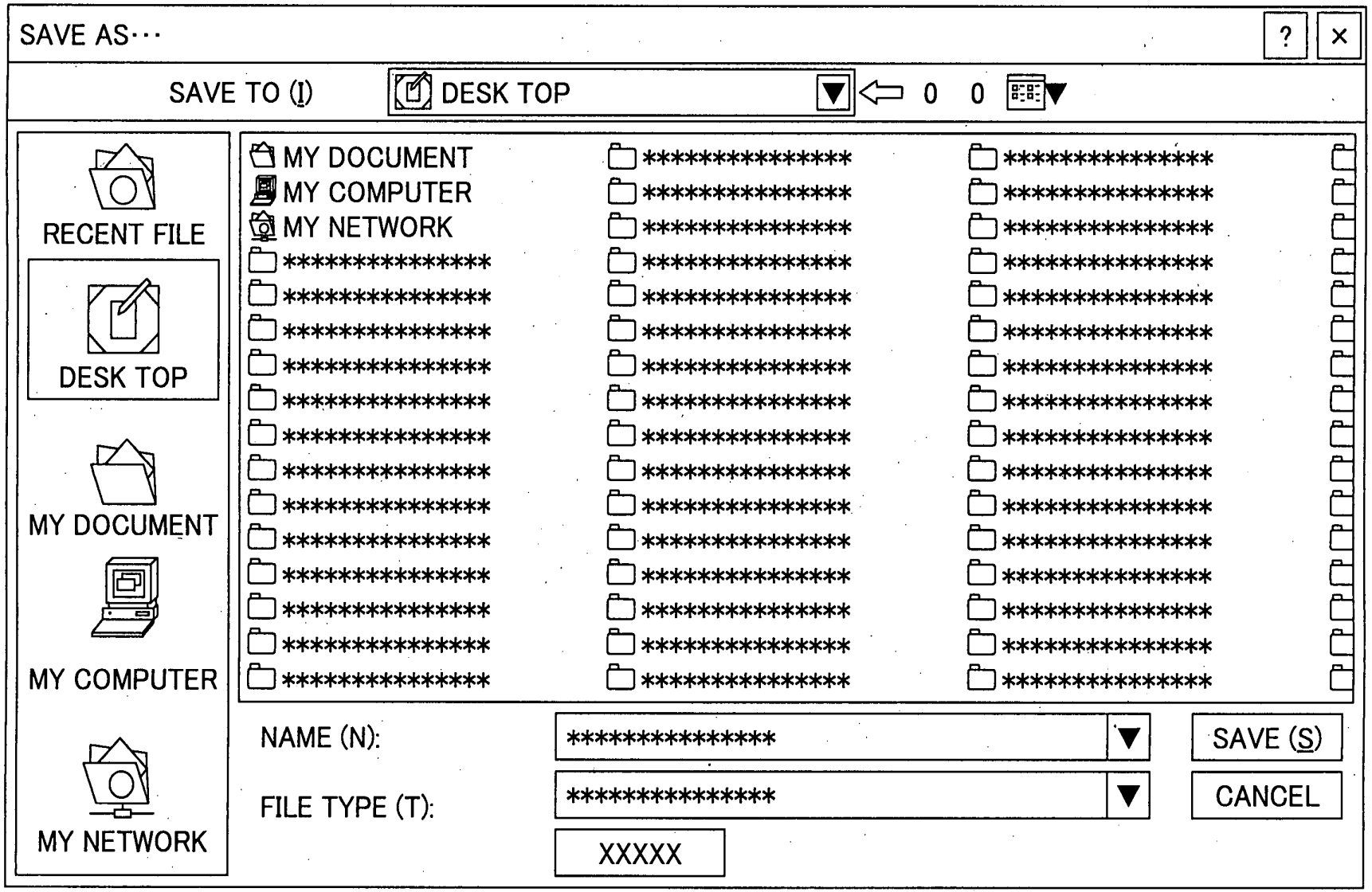

FIG.7

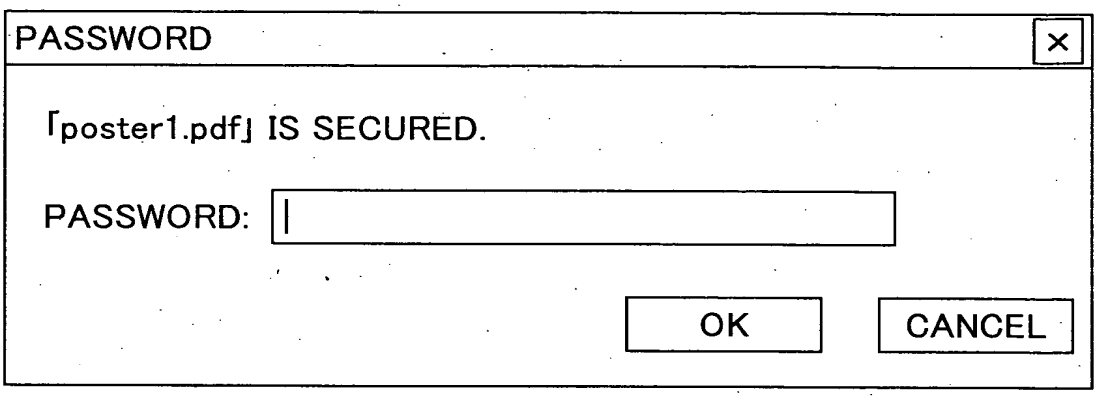

FIG.8

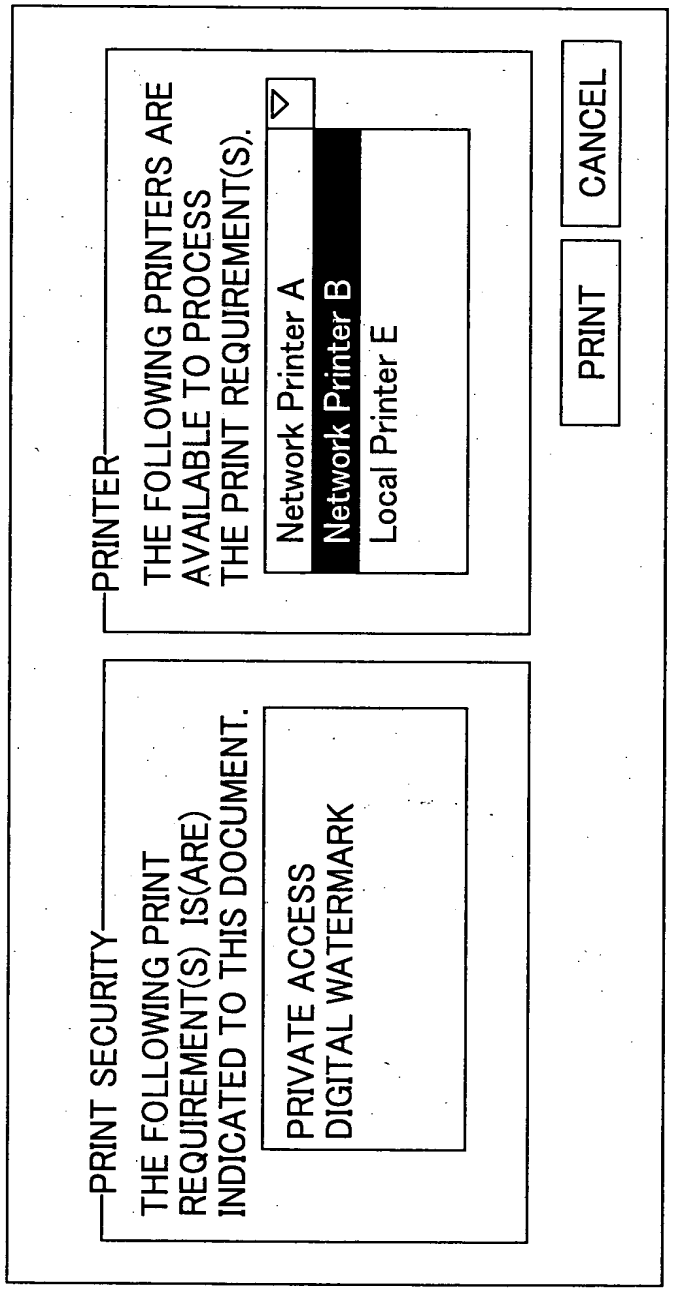
PRINT SECURITY
THE FOLLOWING PRINT REQUIREMENT(S) IS(ARE) INDICATED TO THIS DOCUMENT.
PRIVATE ACCESS
DIGITAL WATERMARK
PRINTER
THE FOLLOWING PRINTERS ARE AVAILABLE TO PROCESS THE PRINT REQUIREMENT(S).
Network Printer A
Network Printer B
Local Printer E
PRINT
CANCEL

FIG.9

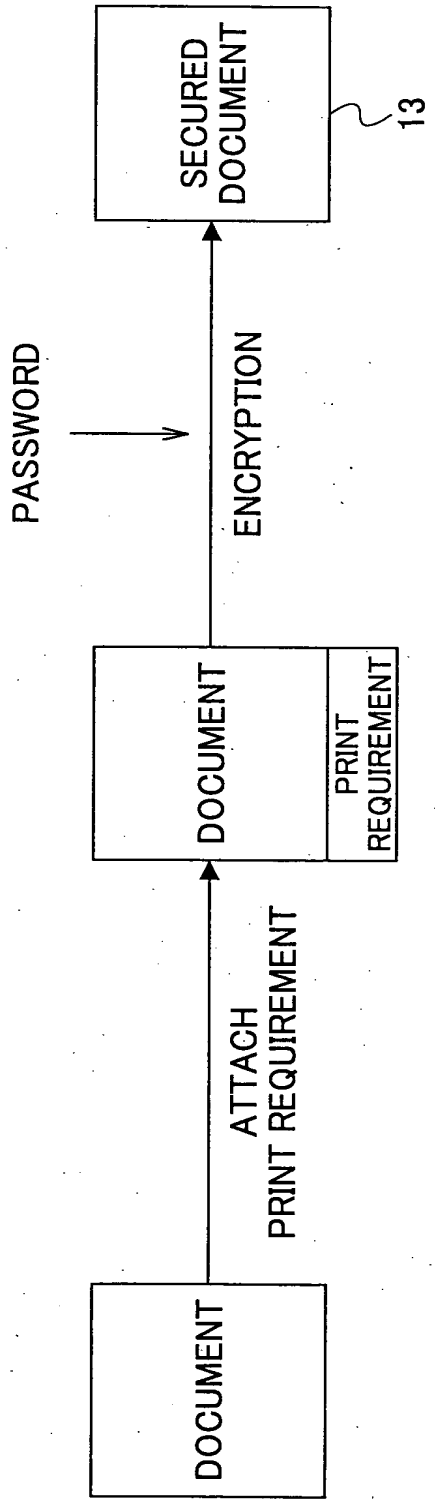
DOCUMENT
ATTACH PRINT REQUIREMENT
DOCUMENT
PRINT REQUIREMENT
PASSWORD
ENCRYPTION
SECURED DOCUMENT
13

FIG.10

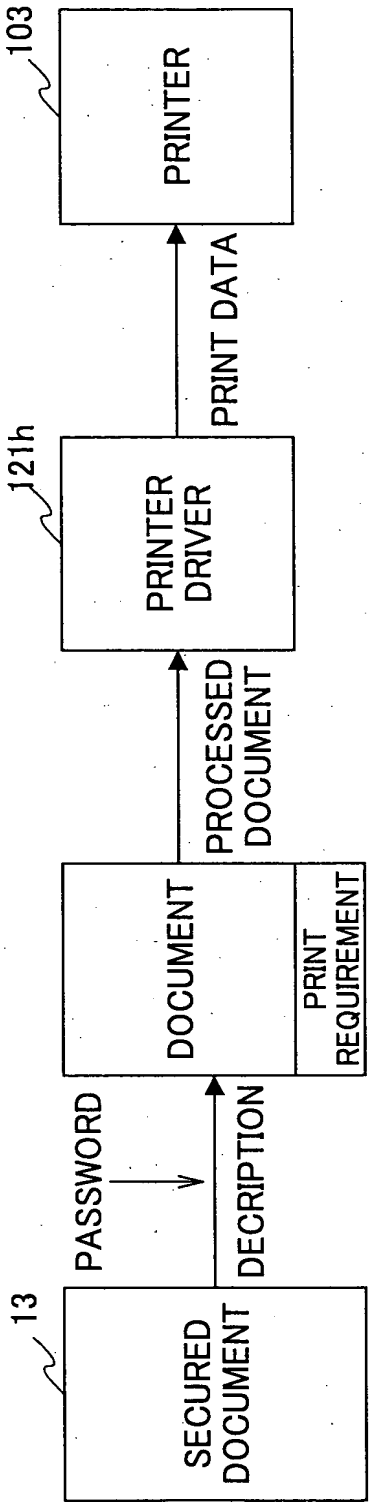
103
PRINTER
PRINT DATA
121h
PRINTER DRIVER
PROCESSED DOCUMENT
DOCUMENT
PRINT REQUIREMENT
PASSWORD
DECRIPTION
13
SECURED DOCUMENT

FIG.11

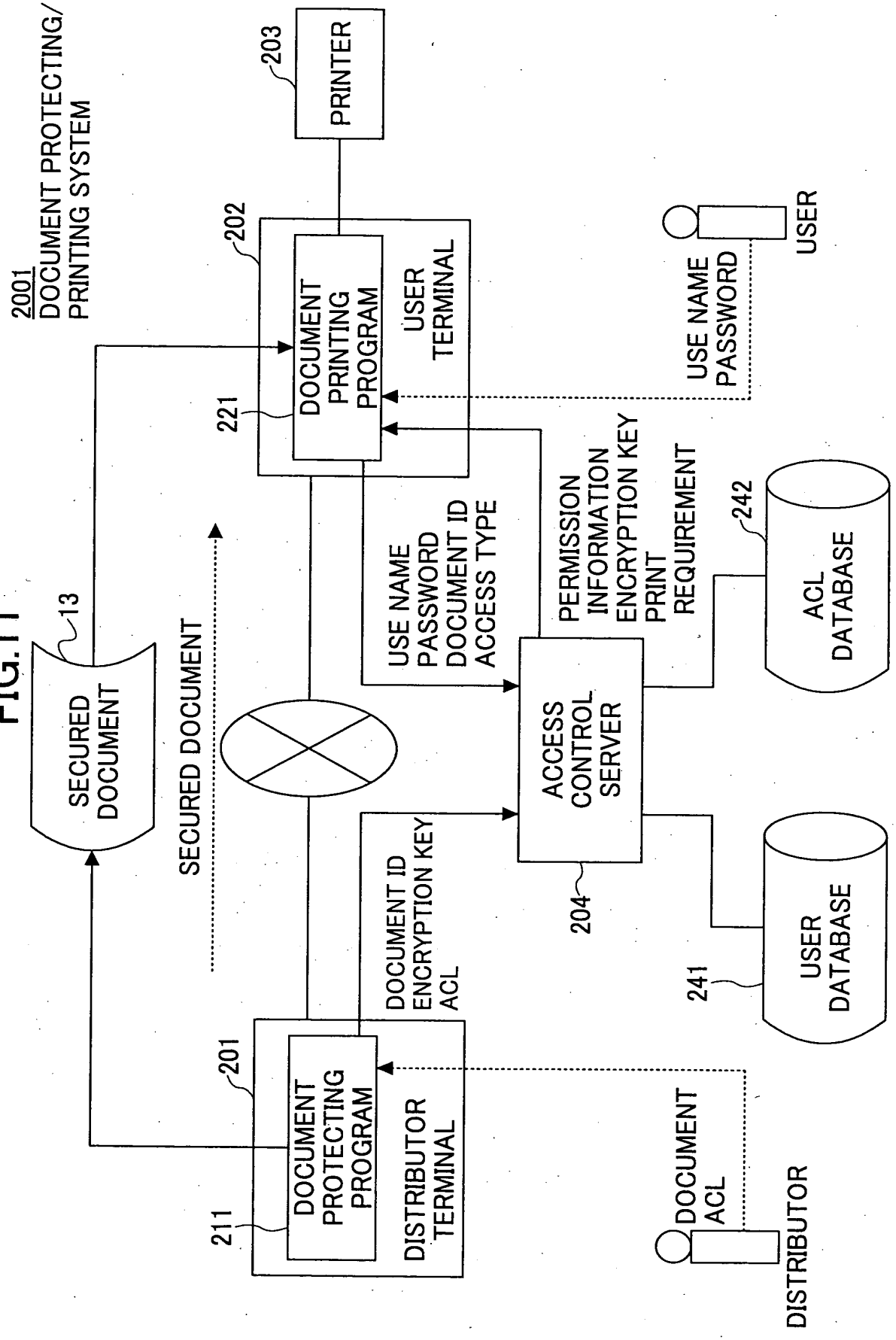
2001
DOCUMENT PROTECTING/
PRINTING SYSTEM
203
PRINTER
202
DOCUMENT
PRINTING
PROGRAM
USER
TERMINAL
221
USE NAME
PASSWORD
USER
13
SECURED
DOCUMENT
SECURED DOCUMENT
USE NAME
PASSWORD
DOCUMENT ID
ACCESS TYPE
PERMISSION
INFORMATION
ENCRYPTION KEY
PRINT
REQUIREMENT
242
ACL
DATABASE
ACCESS
CONTROL
SERVER
204
DOCUMENT ID
ENCRYPTION KEY
ACL
241
USER
DATABASE
201
DOCUMENT
PROTECTING
PROGRAM
DISTRIBUTOR
TERMINAL
211
DOCUMENT
ACL
DISTRIBUTOR

FIG.12

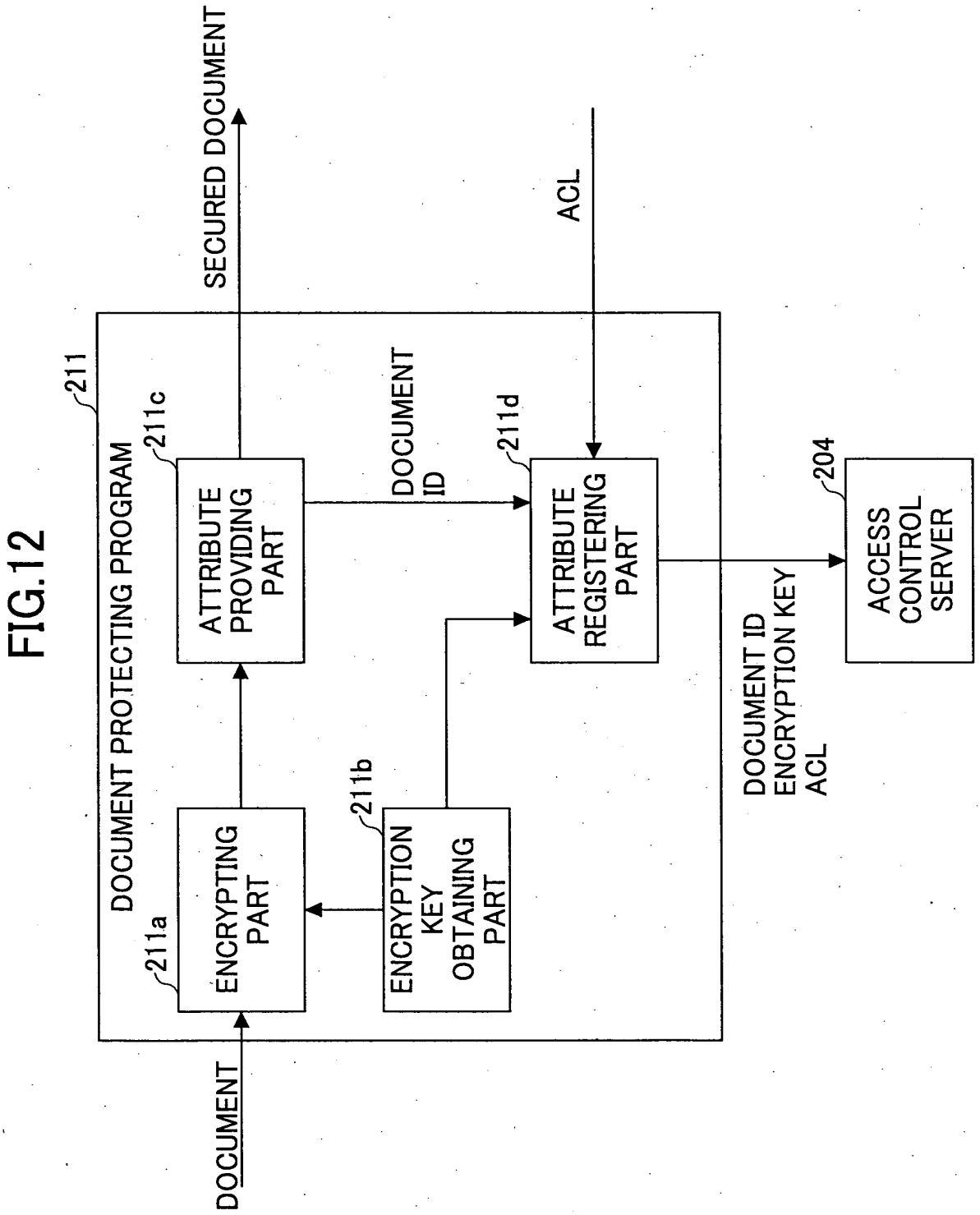
SECURED DOCUMENT
ACL
211
DOCUMENT PROTECTING PROGRAM
211c
ATTRIBUTE PROVIDING PART
DOCUMENT ID
211d
ATTRIBUTE REGISTERING PART
204
ACCESS CONTROL SERVER
DOCUMENT ID ENCRYPTION KEY ACL
211b
ENCRYPTION KEY OBTAINING PART
211a
ENCRYPTING PART
DOCUMENT

FIG.13

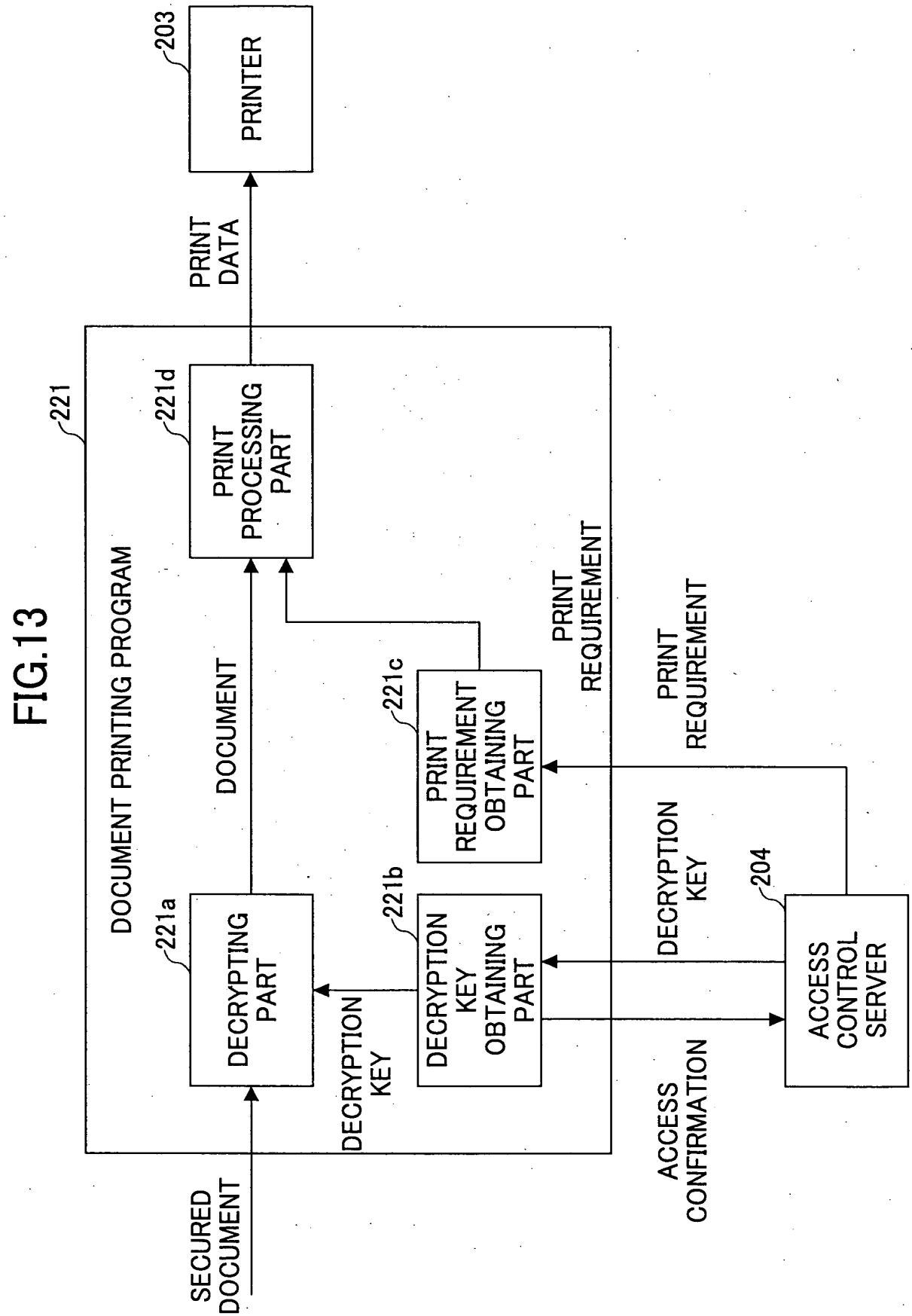
203
PRINTER
PRINT DATA
221
DOCUMENT PRINTING PROGRAM
221d
PRINT PROCESSING PART
DOCUMENT
221c
PRINT REQUIREMENT OBTAINING PART
PRINT REQUIREMENT
PRINT REQUIREMENT
221a
DECRYPTING PART
221b
DECRYPTION KEY OBTAINING PART
DECRYPTION KEY
204
ACCESS CONTROL SERVER
DECRYPTION KEY
ACCESS CONFIRMATION
SECURED DOCUMENT

FIG.14

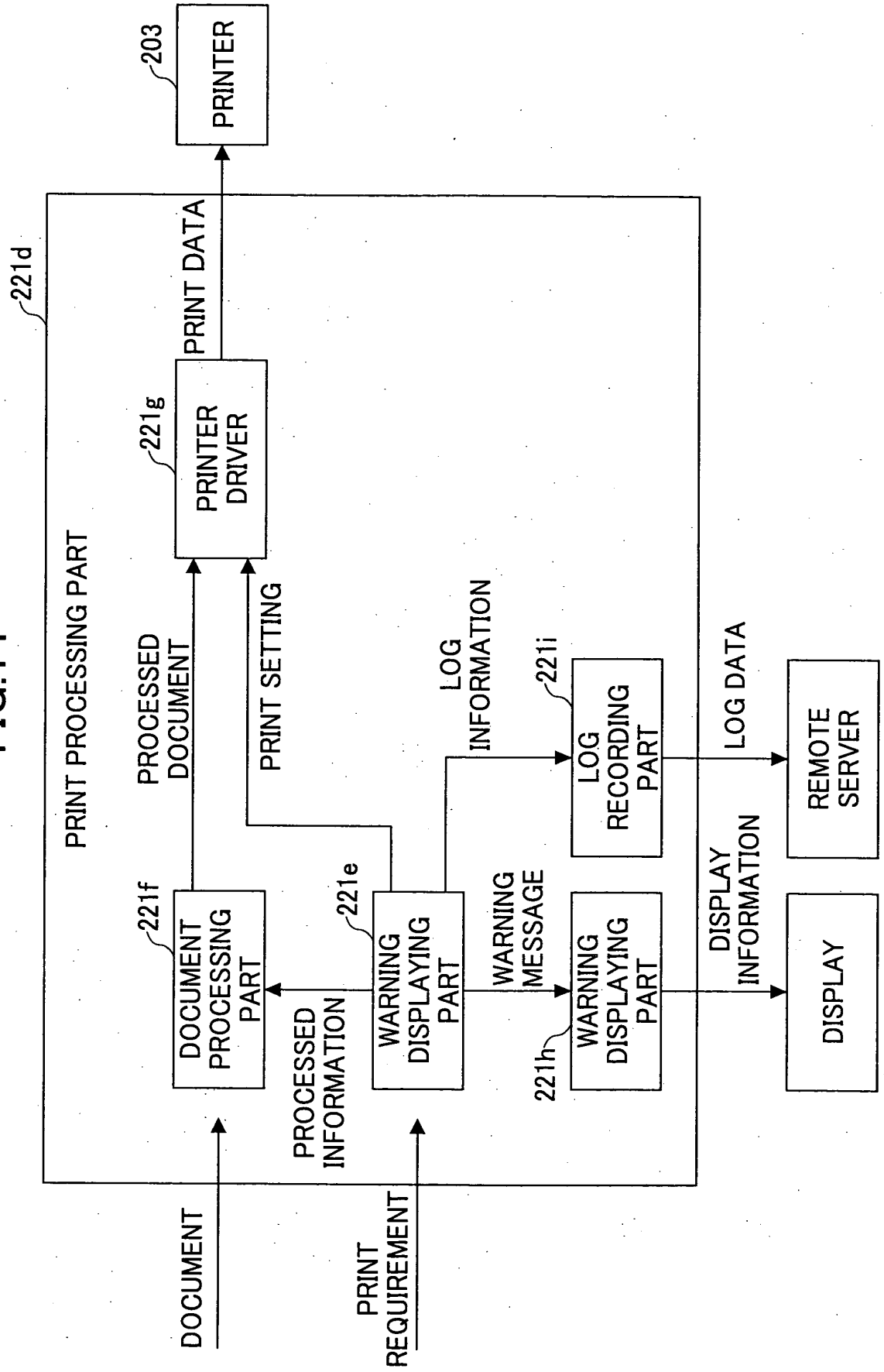
203
PRINTER
221d
PRINT PROCESSING PART
PRINT DATA
221g
PRINTER DRIVER
PROCESSED DOCUMENT
PRINT SETTING
LOG INFORMATION
221i
LOG RECORDING PART
LOG DATA
REMOTE SERVER
221f
DOCUMENT PROCESSING PART
221e
WARNING DISPLAYING PART
WARNING MESSAGE
221h
WARNING DISPLAYING PART
DISPLAY INFORMATION
DISPLAY
PROCESSED INFORMATION
DOCUMENT
PRINT REQUIREMENT

FIG.15

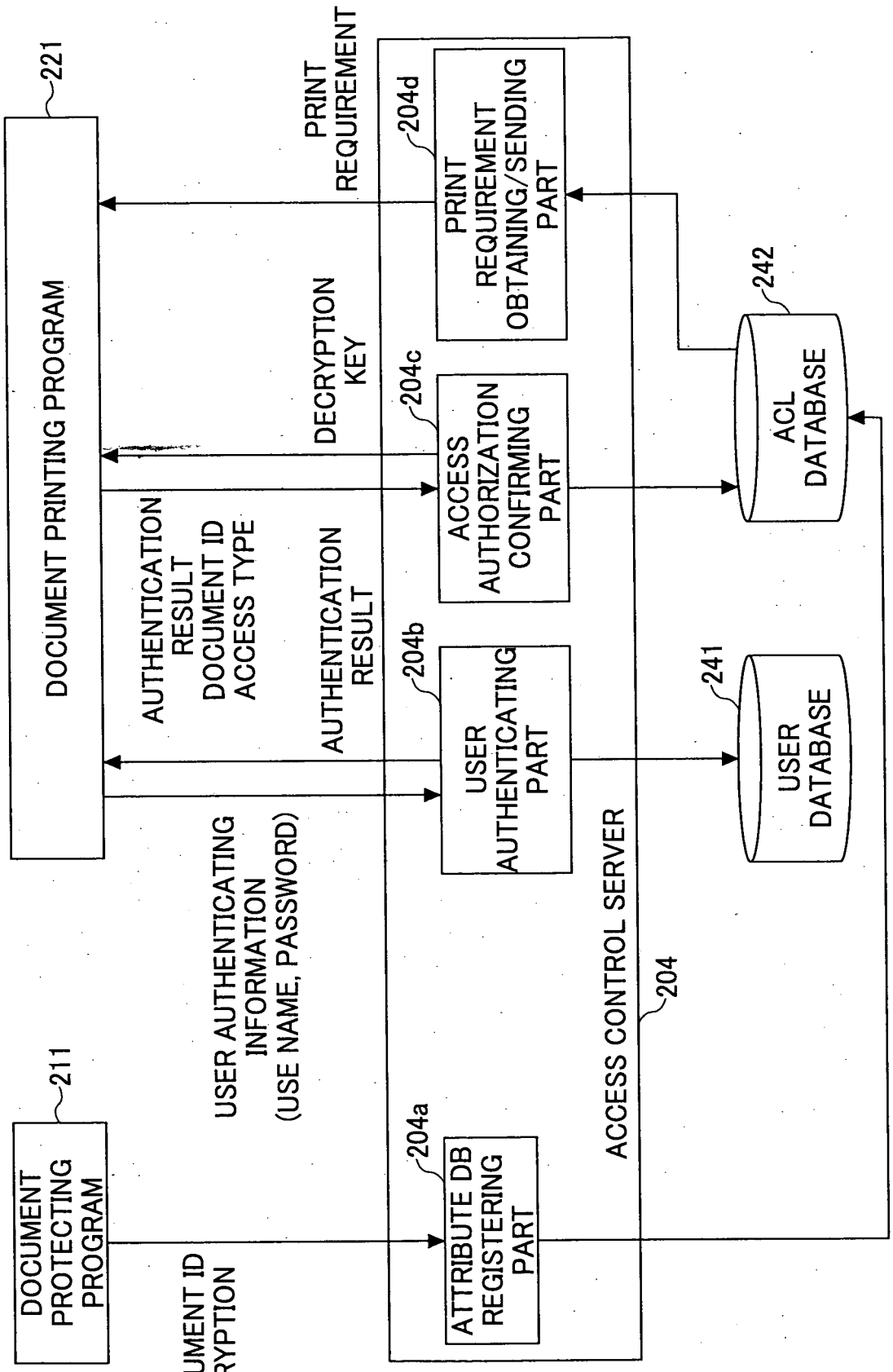
221
DOCUMENT PRINTING PROGRAM
PRINT REQUIREMENT
204d
PRINT REQUIREMENT OBTAINING/SENDING PART
242
ACL DATABASE
DECRYPTION KEY
204c
ACCESS AUTHORIZATION CONFIRMING PART
AUTHENTICATION RESULT
DOCUMENT ID
ACCESS TYPE
AUTHENTICATION RESULT
204b
USER AUTHENTICATING PART
241
USER DATABASE
USER AUTHENTICATING INFORMATION (USE NAME, PASSWORD)
211
DOCUMENT PROTECTING PROGRAM
204a
ATTRIBUTE DB REGISTERING PART
ACCESS CONTROL SERVER
204
DOCUMENT ID
ENCRYPTION KEY
ACL

FIG.16

User name	Access type	Permission	Requirement
Ichiro	Read	Allowed	—
	Write	Denied	—
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Patten)
			EBC(Embedding BarCode)
	Hardcopy	Allowed	RAD(Record Audit Date)
Taro	Read	Allowed	—
	Write	Denied	—
	Print	Denied	—
	Hardcopy	Denied	—
⋮			

FIG.17

Document ID	Key	ACL
133.139.234.23.22.125.98.192	89FECA8D2B	(binary data)
133.139.234.23.22.125.99.105	A73C44DA59	(binary data)

FIG.18

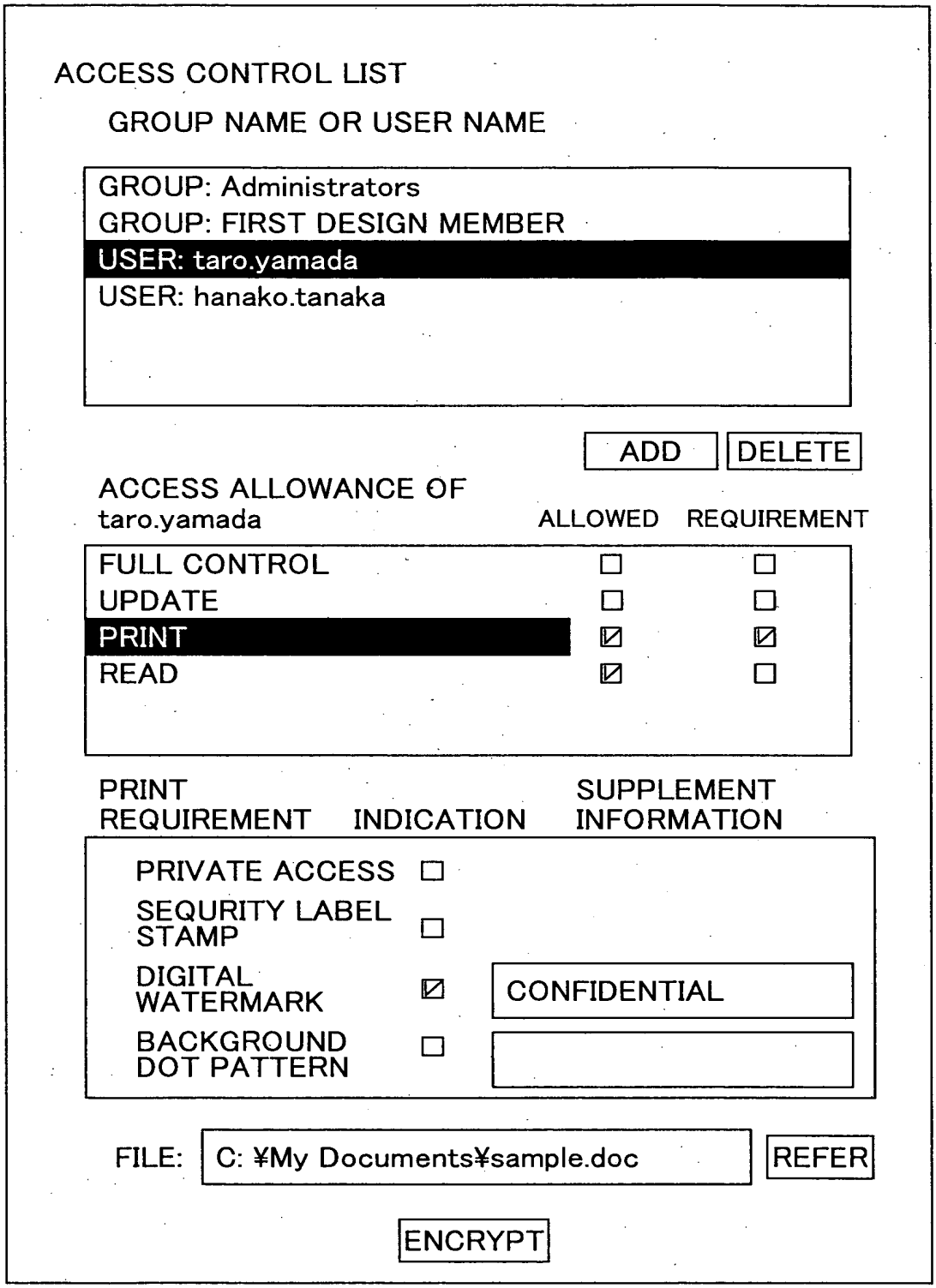
ACCESS CONTROL LIST
GROUP NAME OR USER NAME
GROUP: Administrators
GROUP: FIRST DESIGN MEMBER
USER: taro.yamada
USER: hanako.tanaka
ADD
DELETE
ACCESS ALLOWANCE OF
taro.yamada
ALLOWED
REQUIREMENT
FULL CONTROL
UPDATE
PRINT
READ
PRINT REQUIREMENT
INDICATION
SUPPLEMENT INFORMATION
PRIVATE ACCESS
SEQURITY LABEL STAMP
DIGITAL WATERMARK
CONFIDENTIAL
BACKGROUND DOT PATTERN
FILE:
C: ¥My Documents¥sample.doc
REFER
ENCRYPT

FIG.19

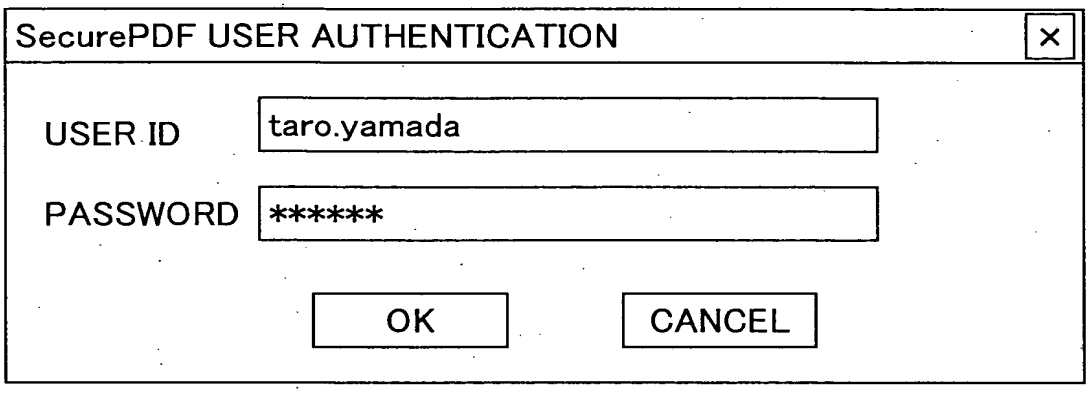
SecurePDF USER AUTHENTICATION
USER ID
taro.yamada
PASSWORD
******
OK
CANCEL

FIG.20

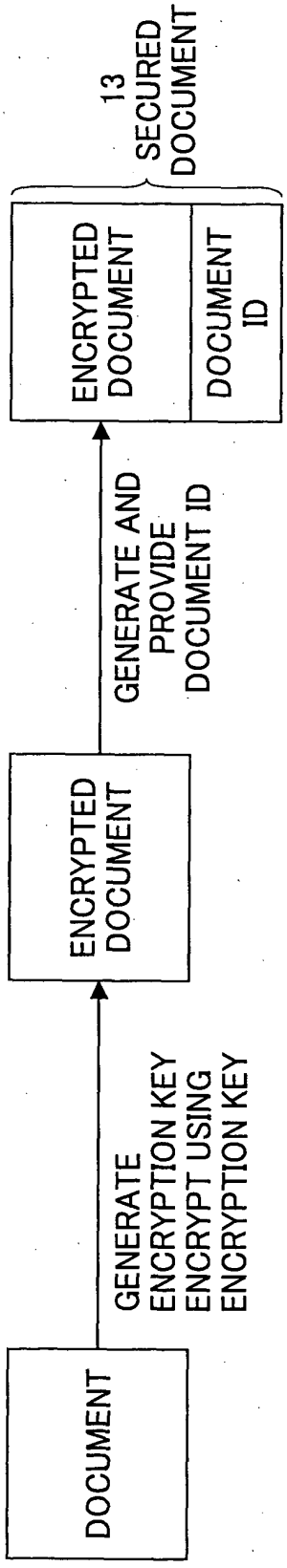
DOCUMENT
GENERATE ENCRYPTION KEY
ENCRYPT USING ENCRYPTION KEY
ENCRYPTED DOCUMENT
GENERATE AND PROVIDE DOCUMENT ID
ENCRYPTED DOCUMENT
DOCUMENT ID
13 SECURED DOCUMENT

FIG.21

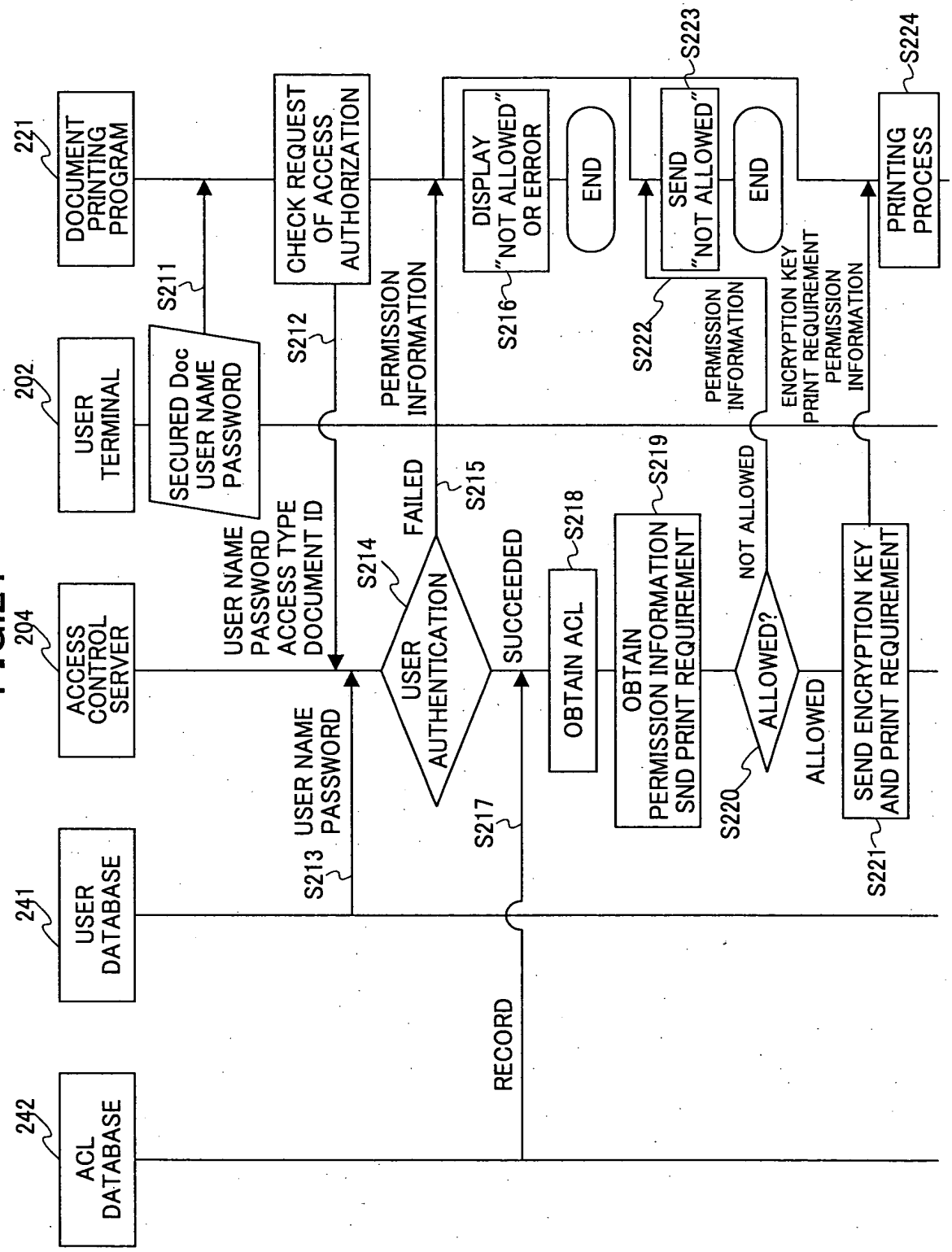
221
DOCUMENT PRINTING PROGRAM
292
USER TERMINAL
204
ACCESS CONTROL SERVER
241
USER DATABASE
242
ACL DATABASE
S211
SECURED Doc USER NAME PASSWORD
USER NAME PASSWORD ACCESS TYPE DOCUMENT ID
S212
CHECK REQUEST OF ACCESS AUTHORIZATION
PERMISSION INFORMATION
S213
USER NAME PASSWORD
S214
USER AUTHENTICATION
FAILED
S215
DISPLAY "NOT ALLOWED" OR ERROR
S216
END
SUCCEEDED
S217
RECORD
S218
OBTAIN ACL
S219
OBTAIN PERMISSION INFORMATION SND PRINT REQUIREMENT
S220
ALLOWED?
NOT ALLOWED
S222
SEND "NOT ALLOWED"
S223
END
PERMISSION INFORMATION
ALLOWED
S221
SEND ENCRYPTION KEY AND PRINT REQUIREMENT
ENCRYPTION KEY PRINT REQUIREMENT PERMISSION INFORMATION
S224
PRINTING PROCESS

FIG.22

291

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
 s:encodingStyle="http://shemas.xmlsoap.org/soap/encoding/">
<s:Body>
<m:isAllowed xmlns:m="http://sample.com/sample">
<sessionId>adfkla;iowoemads</sessionId>
<userId>taro.yamada</userId>
<docId>shm000000000003</docId>
<accessType>print</accessType>
</m:isAllowed>
</s:Body>
</s:Envelope>
```

292

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://shemas.xmlsoap.org/soap/encoding/">
<s:Body>
<m:isAllowedResponse xmlns:ns1="http://sample.com/sample">
<isAllowedReturn>
<allowed xsi:type="xsd:boolean">true</allowed>
<requirements>
<item>
<requirement>private_access</requirement>
</item>
<item>
<requirement>watermark</requirement>
<supplement>CONFIDENTIAL</supplement>
</item>
</requirements>
</isAllowedReturn>
</m:isAllowedResponse>
</s:Body>
</s:Envelope>
```

FIG.23

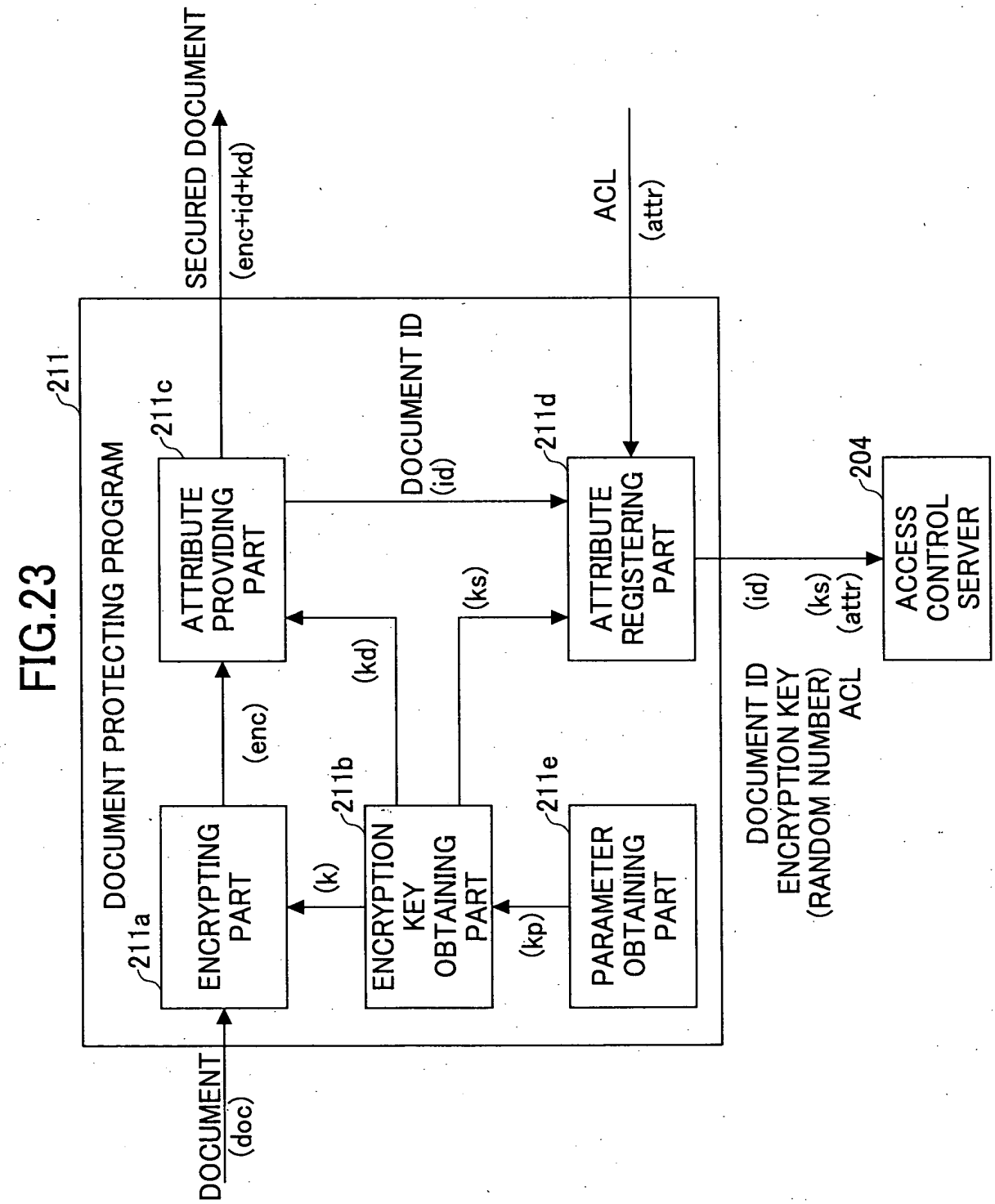
DOCUMENT (doc)
211
DOCUMENT PROTECTING PROGRAM
211a
ENCRYPTING PART
(enc)
211b
ENCRYPTION KEY OBTAINING PART
(k)
(kd)
211c
ATTRIBUTE PROVIDING PART
(kp)
211e
PARAMETER OBTAINING PART
SECURED DOCUMENT
(enc+id+kd)
DOCUMENT ID
(id)
(ks)
211d
ATTRIBUTE REGISTERING PART
ACL
(attr)
DOCUMENT ID
ENCRYPTION KEY
(RANDOM NUMBER)
ACL
(id)
(ks)
(attr)
204
ACCESS CONTROL SERVER

FIG.24

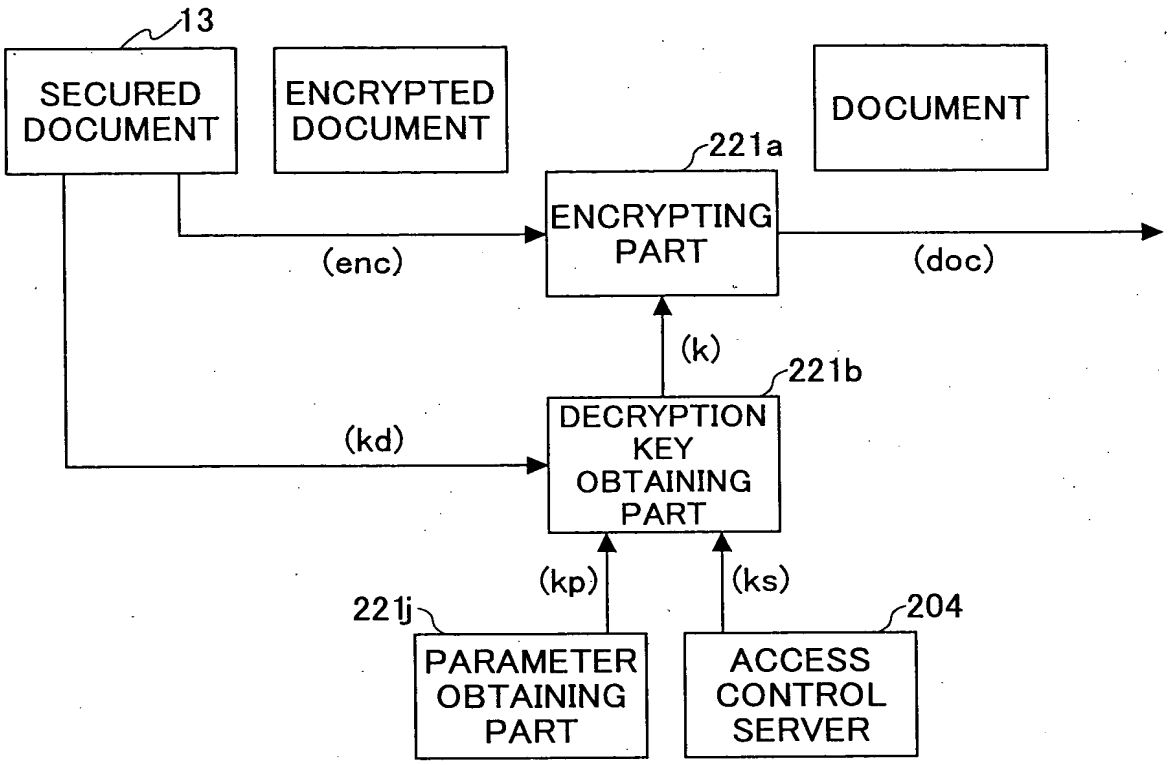
13
SECURED DOCUMENT
ENCRYPTED DOCUMENT
DOCUMENT
221a
ENCRYPTING PART
(enc)
(doc)
(k)
221b
DECRYPTION KEY OBTAINING PART
(kd)
(kp)
(ks)
221j
PARAMETER OBTAINING PART
204
ACCESS CONTROL SERVER

FIG.25

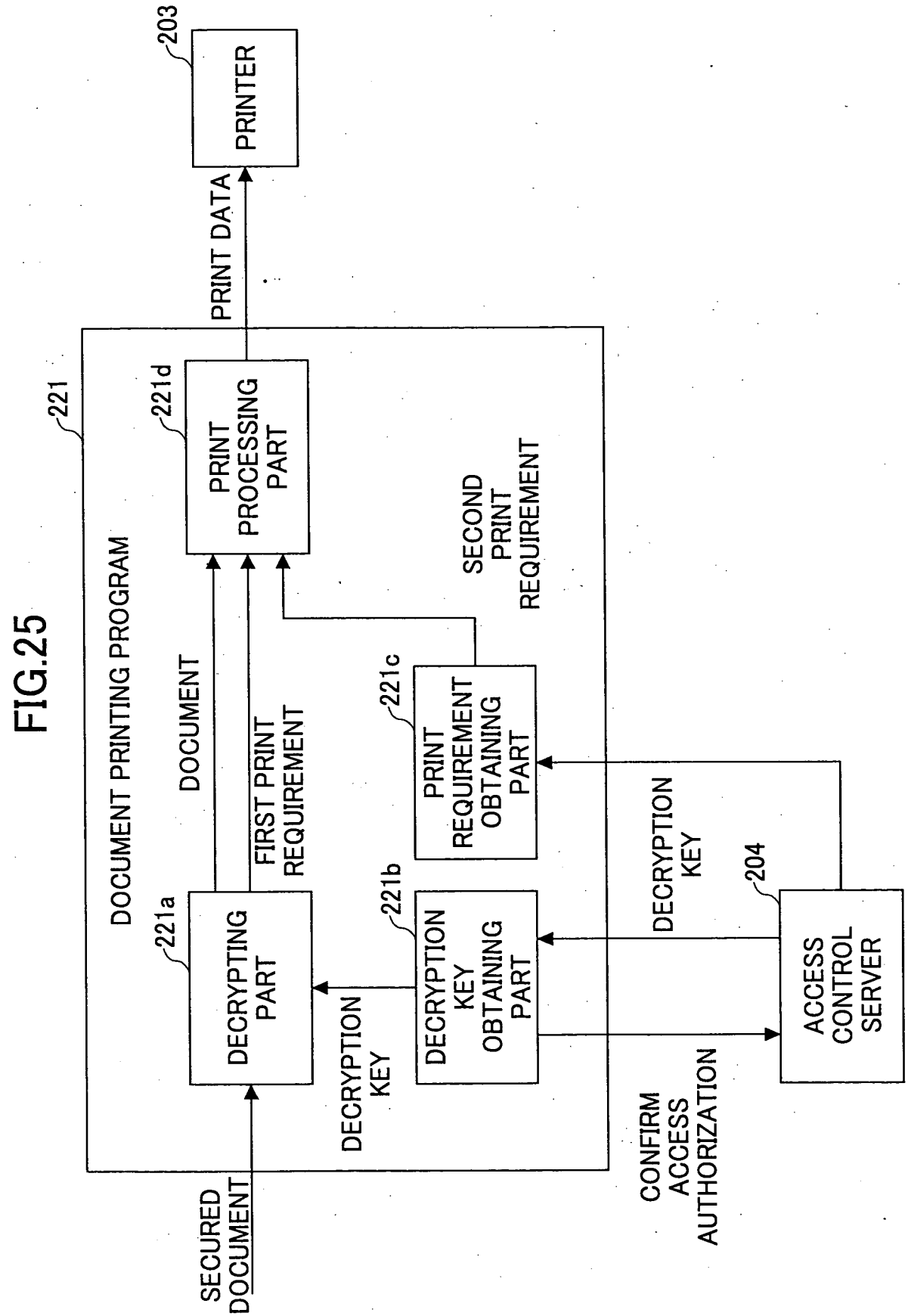
203
PRINTER
PRINT DATA
221
DOCUMENT PRINTING PROGRAM
221d
PRINT PROCESSING PART
SECOND PRINT REQUIREMENT
DOCUMENT
FIRST PRINT REQUIREMENT
221c
PRINT REQUIREMENT OBTAINING PART
221a
DECRYPTING PART
221b
DECRYPTION KEY OBTAINING PART
DECRYPTION KEY
204
ACCESS CONTROL SERVER
DECRYPTION KEY
CONFIRM ACCESS AUTHORIZATION
SECURED DOCUMENT

FIG.26

PRINT SECURITY FUNCTIONS

SECURITY LABEL STAMP	FUNCTION FOR PRINTING BY OVERLAPPING MANUSCRIPT WITH A MARK SHOWING "SECRET" AS STAMP OR WATERMARK AT GIVEN LOCATION IN PAGE. BITMAP IMAGE OR CHARACTER STRING SUCH AS "SECRET", "CONFIDENTIAL", OR A LIKE CAN BE USED AS STAMP.
BACKGROUND DOT PATTERN	FUNCTION FOR PRINTING BY OVERLAPPING MANUSCRIPT WITH BACKGROUND IMAGE THAT IS CONTROLLED SO THAT THE A SPECIAL IMAGE IS RAISED WHEN COPIER COPIES. IN GENERAL, IMAGE INDICATED AS STAMP IN ABOVE STAMP FUNCTION IS USED TO BE BACKGROUND IMAGE.
PRIVATE ACCESS	FUNCTION FOR PRINTING OUT UNTIL USER COMES TO PRINTER AND INPUTS PIN (PERSONAL IDENTIFICATION NUMBER) TO OPERATION PANEL OF PRINTER IF USER INDICATES PIN TO PRINTER DRIVER WHEN INDICATING TO PRINT OUT

FIG.27

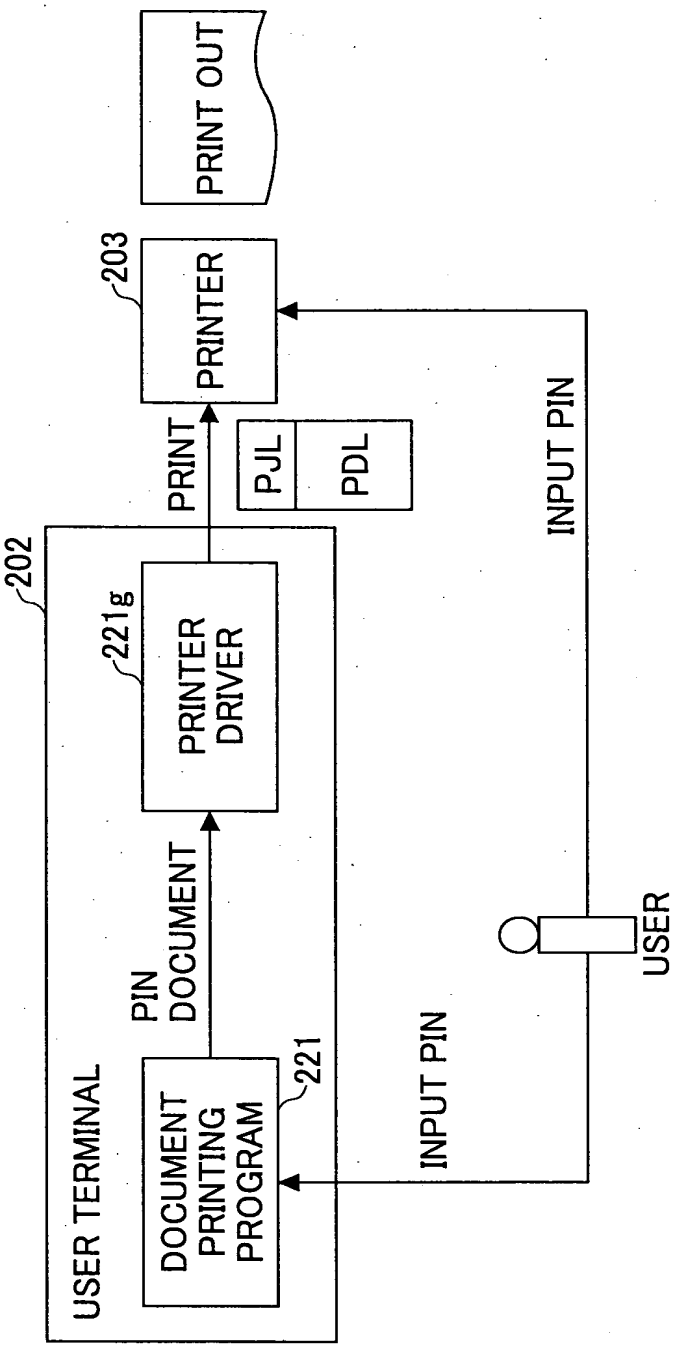
PRINT OUT
203
PRINTER
PRINT
PJL
PDL
202
221g
PRINTER DRIVER
INPUT PIN
PIN DOCUMENT
USER TERMINAL
DOCUMENT PRINTING PROGRAM
221
INPUT PIN
USER

FIG.28

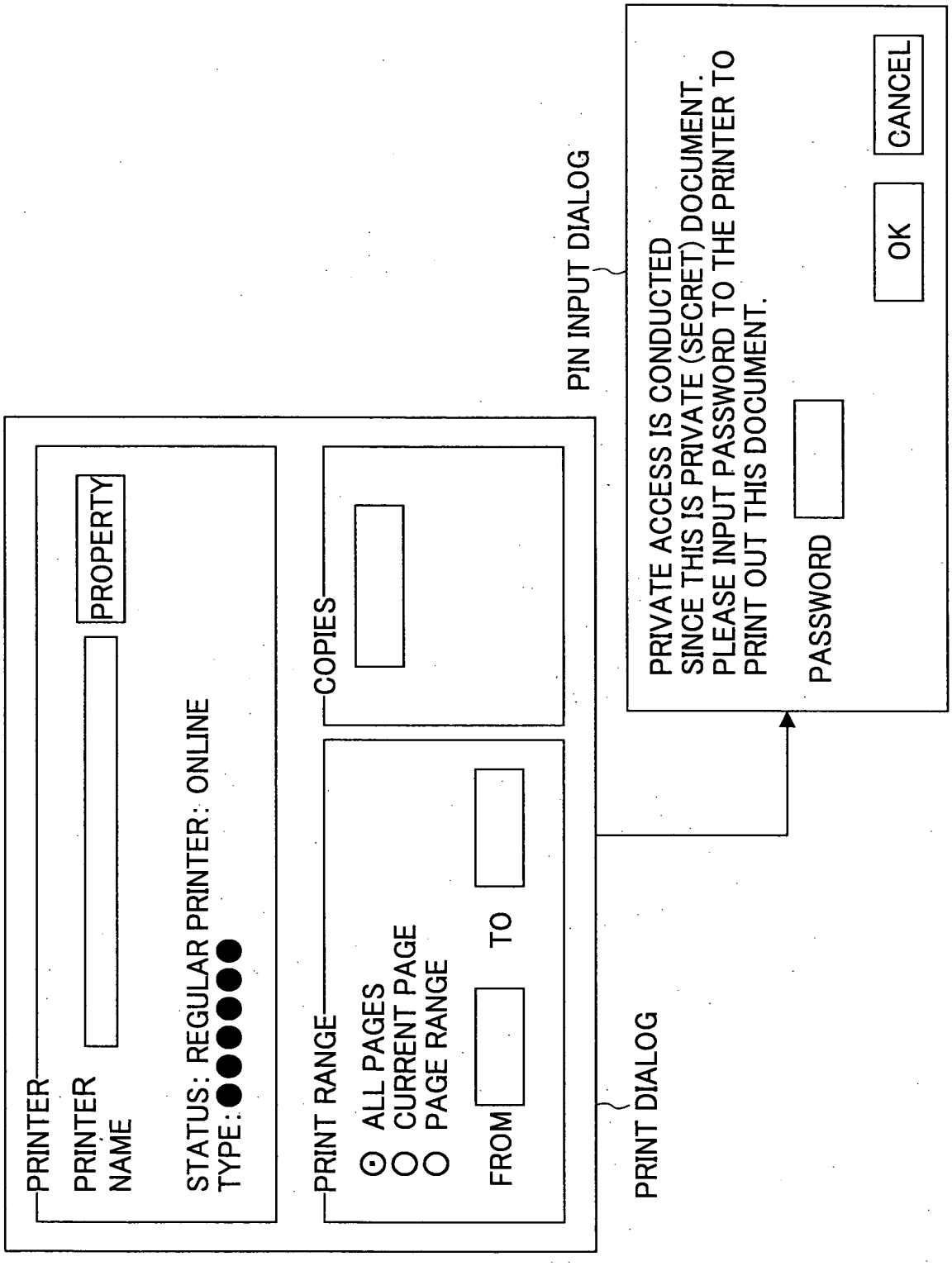
PRINTER
PRINTER NAME
PROPERTY
STATUS: REGULAR PRINTER: ONLINE
TYPE:
COPIES
PRINT RANGE
ALL PAGES
CURRENT PAGE
PAGE RANGE
FROM
TO
PRINT DIALOG
PIN INPUT DIALOG
PRIVATE ACCESS IS CONDUCTED
SINCE THIS IS PRIVATE (SECRET) DOCUMENT.
PLEASE INPUT PASSWORD TO THE PRINTER TO
PRINT OUT THIS DOCUMENT.
PASSWORD
OK
CANCEL

FIG.29

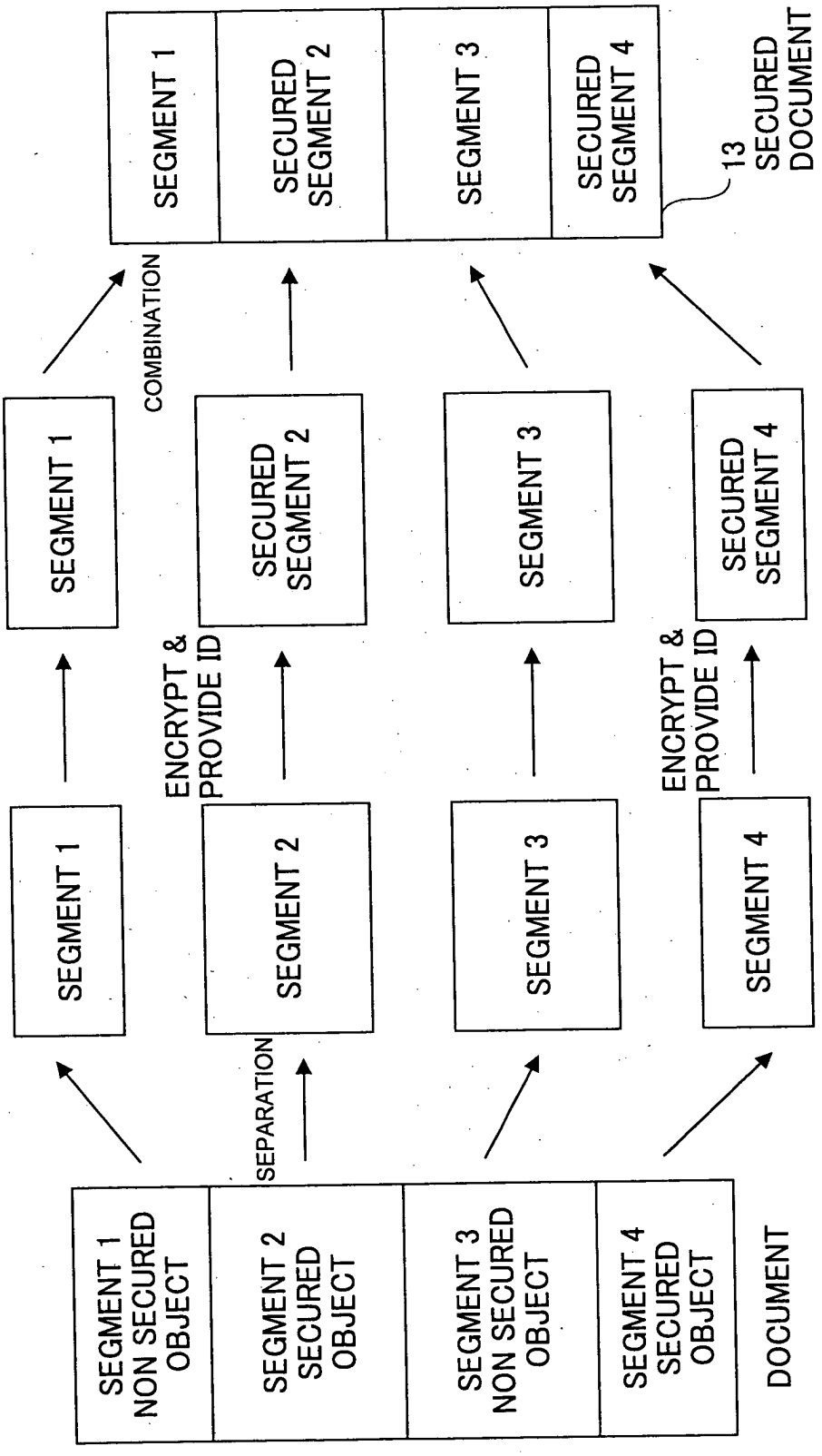
SEGMENT 1
NON SECURED OBJECT
SEGMENT 2
SECURED OBJECT
SEGMENT 3
NON SECURED OBJECT
SEGMENT 4
SECURED OBJECT
DOCUMENT
SEPARATION
SEGMENT 1
SEGMENT 2
SEGMENT 3
SEGMENT 4
ENCRYPT & PROVIDE ID
ENCRYPT & PROVIDE ID
SEGMENT 1
SECURED SEGMENT 2
SEGMENT 3
SECURED SEGMENT 4
COMBINATION
SEGMENT 1
SECURED SEGMENT 2
SEGMENT 3
SECURED SEGMENT 4
13
SECURED DOCUMENT

FIG.30

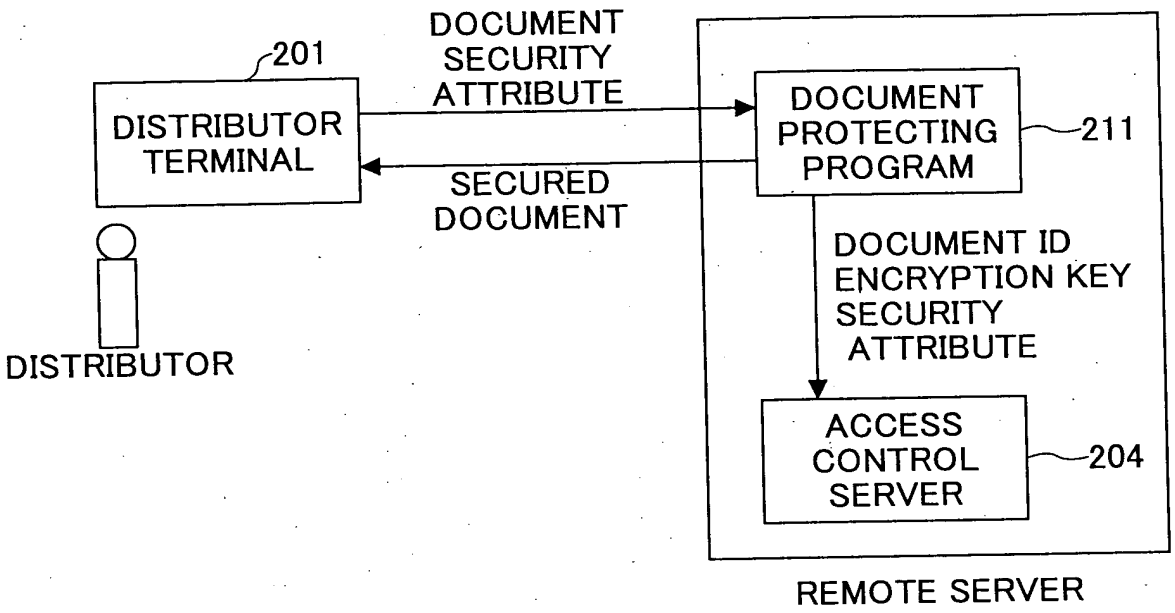
201
DISTRIBUTOR TERMINAL
DISTRIBUTOR
DOCUMENT SECURITY ATTRIBUTE
SECURED DOCUMENT
DOCUMENT PROTECTING PROGRAM
211
DOCUMENT ID
ENCRYPTION KEY
SECURITY ATTRIBUTE
ACCESS CONTROL SERVER
204
REMOTE SERVER

FIG.31

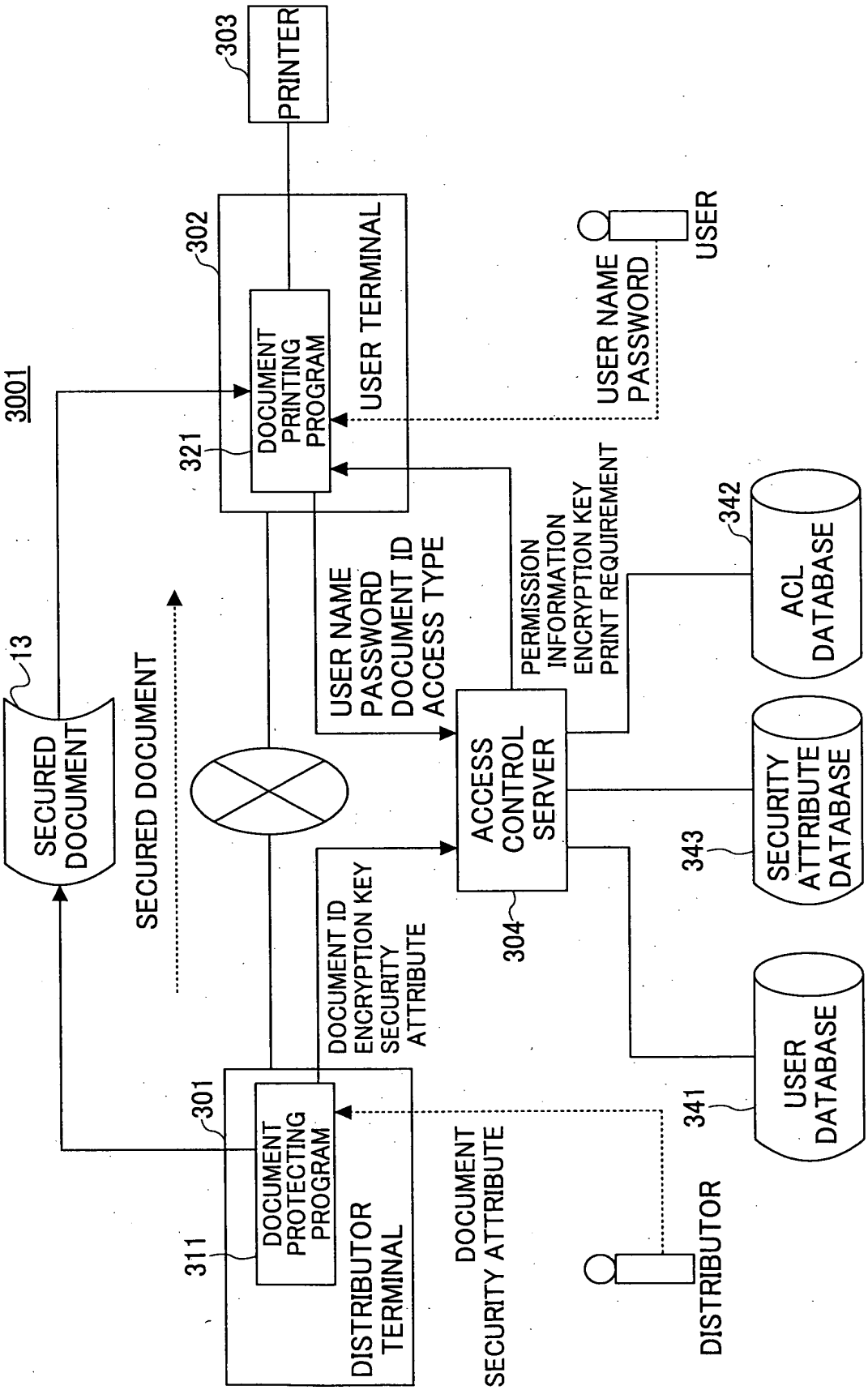
3001
303
PRINTER
302
USER TERMINAL
DOCUMENT PRINTING PROGRAM
321
USER NAME PASSWORD
USER
13
SECURED DOCUMENT
SECURED DOCUMENT
USER NAME
PASSWORD
DOCUMENT ID
ACCESS TYPE
PERMISSION INFORMATION
ENCRYPTION KEY
PRINT REQUIREMENT
342
ACL DATABASE
ACCESS CONTROL SERVER
304
343
SECURITY ATTRIBUTE DATABASE
DOCUMENT ID
ENCRYPTION KEY
SECURITY ATTRIBUTE
301
DOCUMENT PROTECTING PROGRAM
311
DISTRIBUTOR TERMINAL
DOCUMENT SECURITY ATTRIBUTE
341
USER DATABASE
DISTRIBUTOR

FIG.32

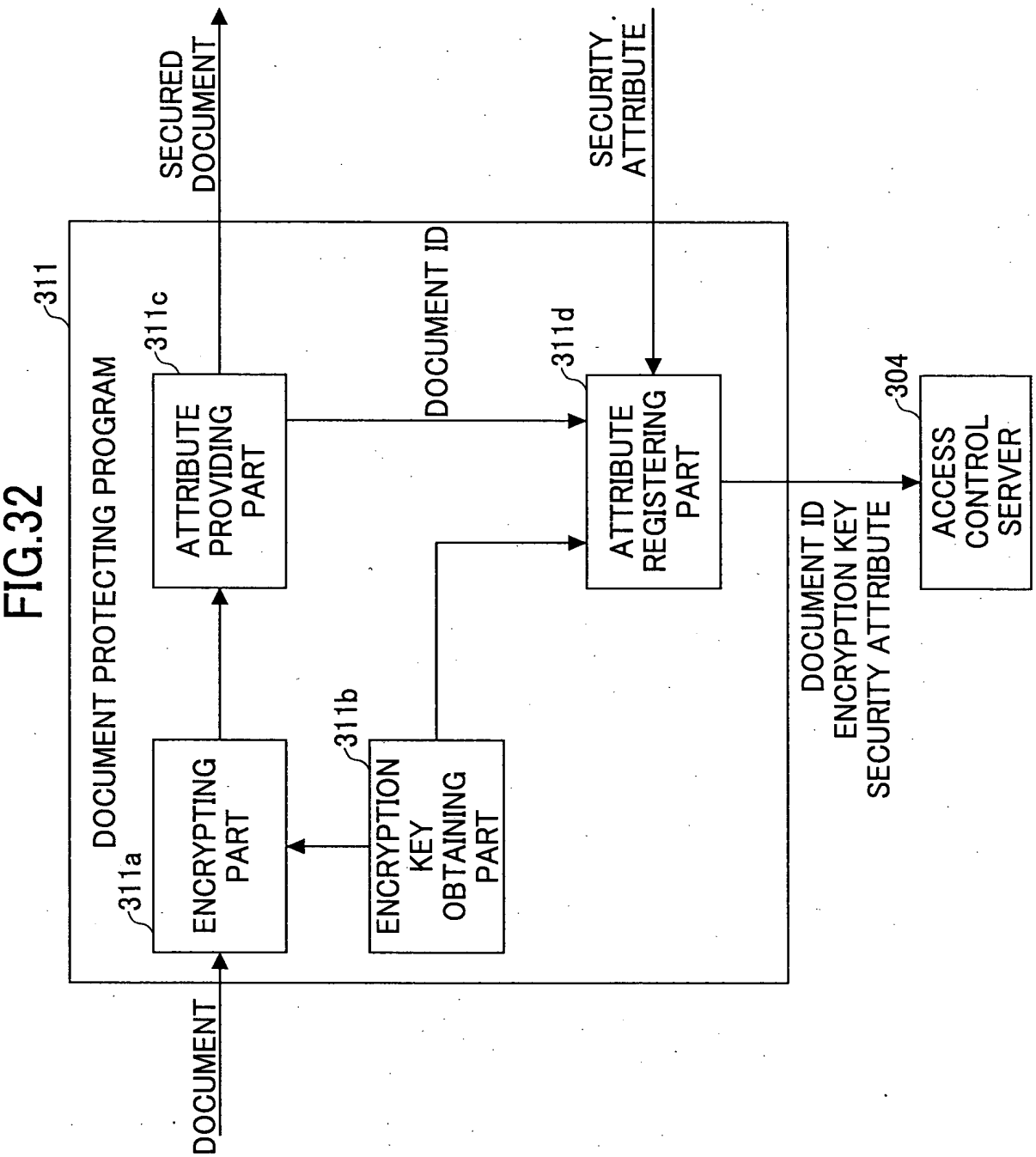
DOCUMENT
SECURED DOCUMENT
SECURITY ATTRIBUTE
311
DOCUMENT PROTECTING PROGRAM
311a
ENCRYPTING PART
311b
ENCRYPTION KEY OBTAINING PART
311c
ATTRIBUTE PROVIDING PART
DOCUMENT ID
311d
ATTRIBUTE REGISTERING PART
DOCUMENT ID
ENCRYPTION KEY
SECURITY ATTRIBUTE
304
ACCESS CONTROL SERVER

FIG.33

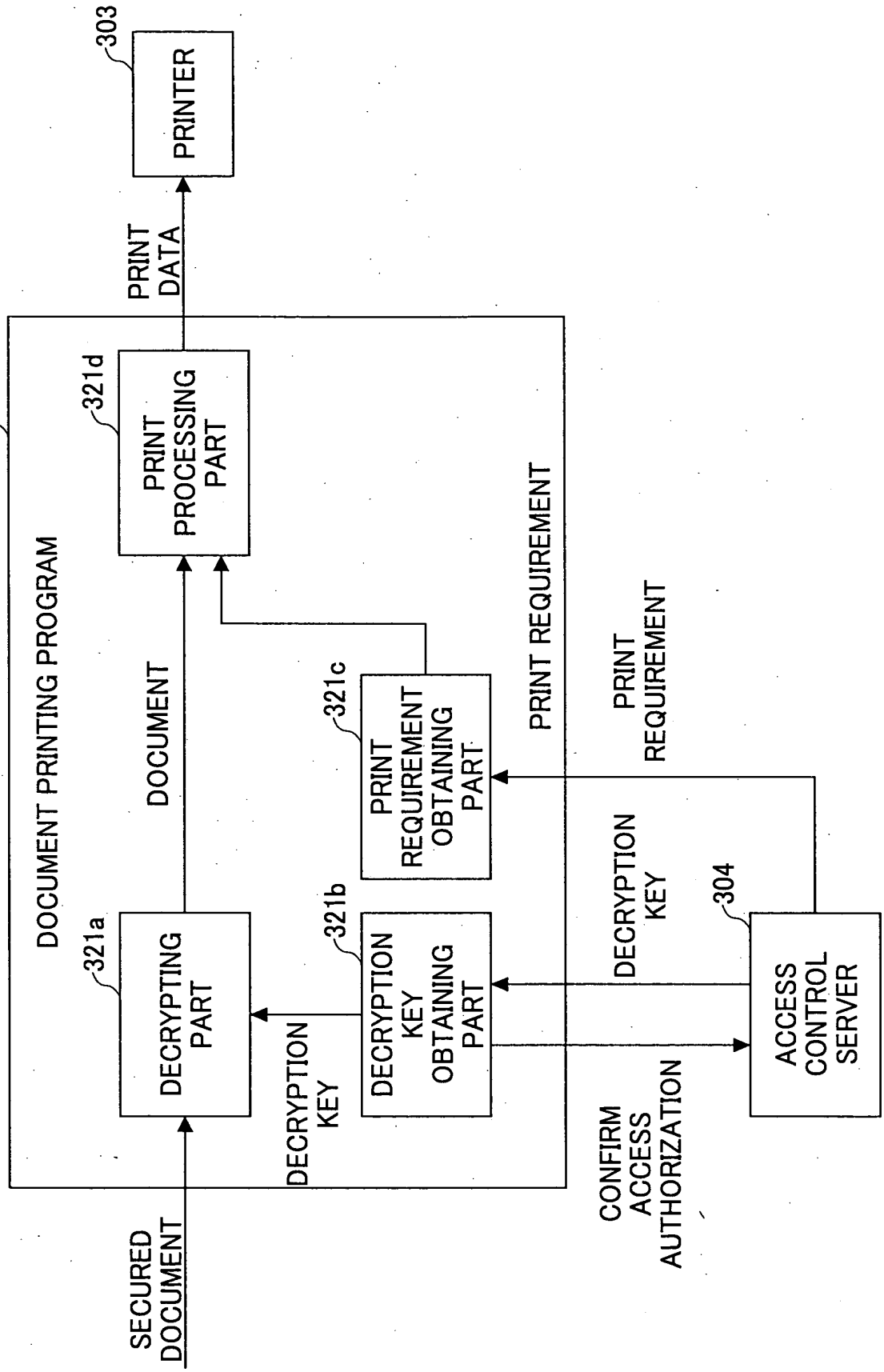
303
PRINTER
PRINT DATA
321
DOCUMENT PRINTING PROGRAM
321d
PRINT PROCESSING PART
DOCUMENT
321c
PRINT REQUIREMENT OBTAINING PART
PRINT REQUIREMENT
321a
DECRYPTING PART
321b
DECRYPTION KEY OBTAINING PART
DECRYPTION KEY
304
ACCESS CONTROL SERVER
DECRYPTION KEY
CONFIRM ACCESS AUTHORIZATION
SECURED DOCUMENT

FIG.34

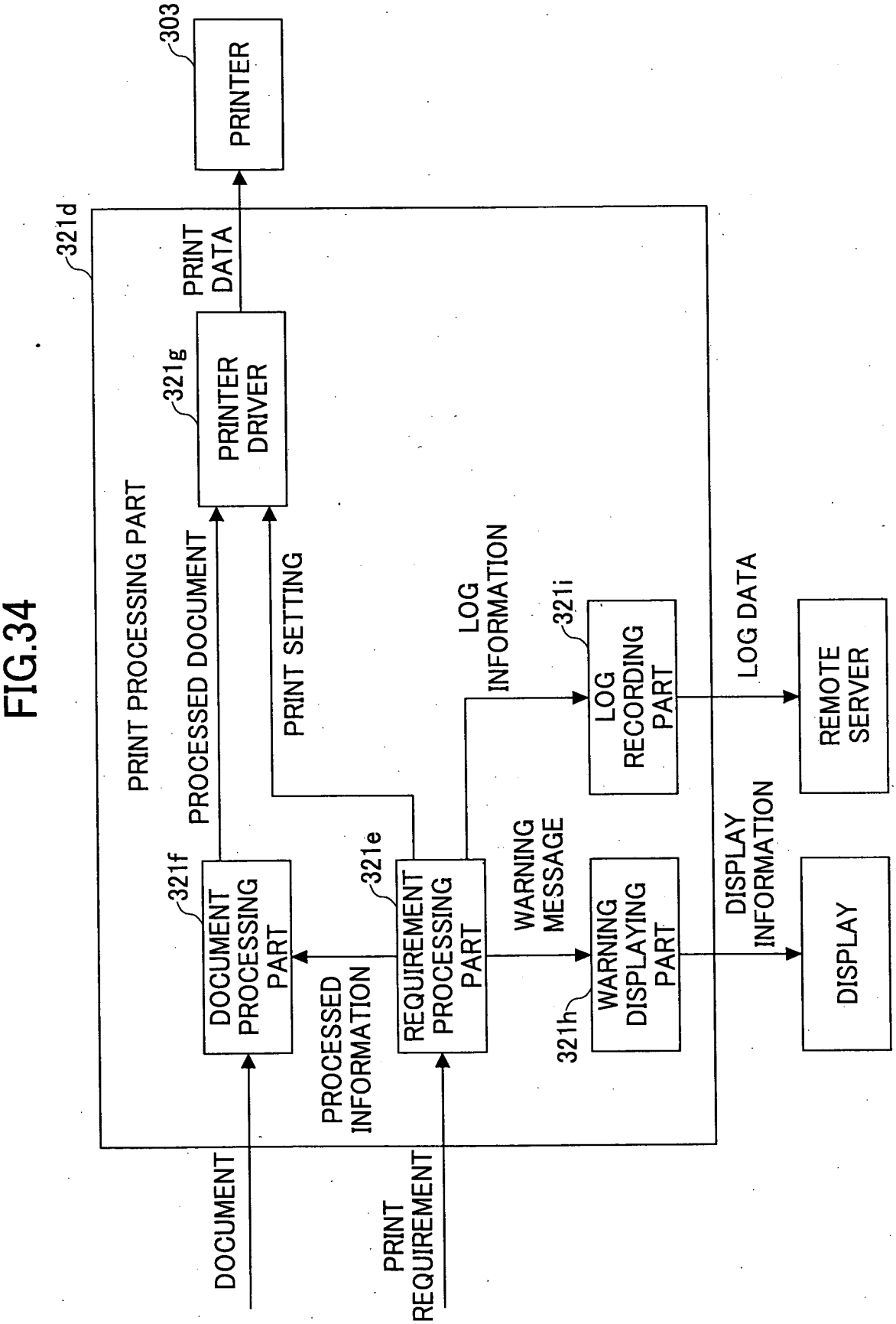
303
PRINTER
321d
PRINT PROCESSING PART
PRINT DATA
321g
PRINTER DRIVER
PROCESSED DOCUMENT
PRINT SETTING
LOG INFORMATION
321i
LOG RECORDING PART
LOG DATA
REMOTE SERVER
321f
DOCUMENT PROCESSING PART
321e
REQUIREMENT PROCESSING PART
WARNING MESSAGE
321h
WARNING DISPLAYING PART
DISPLAY INFORMATION
DISPLAY
PROCESSED INFORMATION
DOCUMENT
PRINT REQUIREMENT

FIG.35

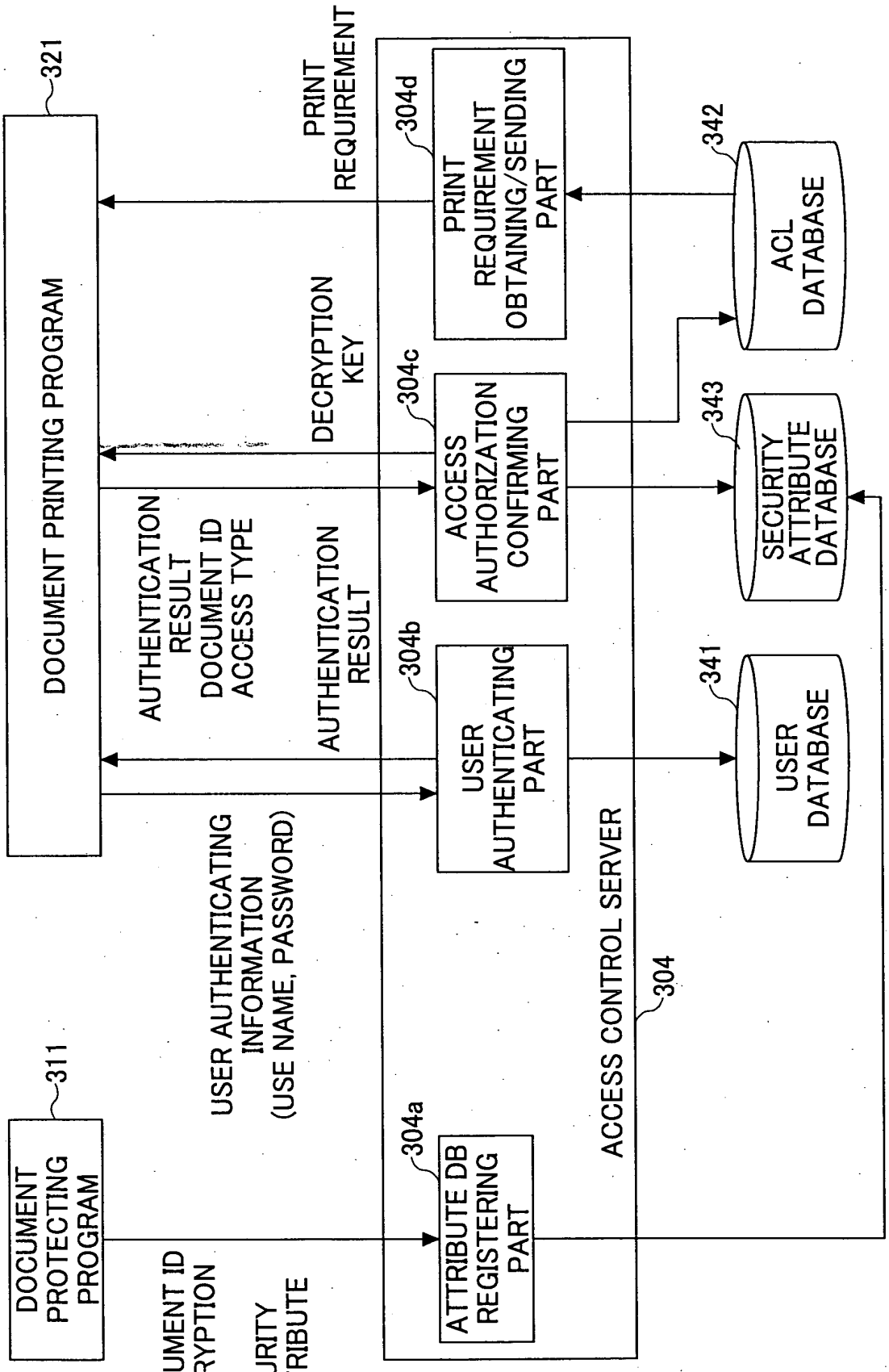
321
DOCUMENT PRINTING PROGRAM
PRINT REQUIREMENT
304d
PRINT REQUIREMENT OBTAINING/SENDING PART
342
ACL DATABASE
DECRYPTION KEY
304c
ACCESS AUTHORIZATION CONFIRMING PART
343
SECURITY ATTRIBUTE DATABASE
AUTHENTICATION RESULT
DOCUMENT ID ACCESS TYPE
AUTHENTICATION RESULT
304b
USER AUTHENTICATING PART
341
USER DATABASE
USER AUTHENTICATING INFORMATION (USE NAME, PASSWORD)
ACCESS CONTROL SERVER
304
311
DOCUMENT PROTECTING PROGRAM
304a
ATTRIBUTE DB REGISTERING PART
DOCUMENT ID
ENCRYPTION KEY
SECURITY ATTRIBUTE

FIG.36

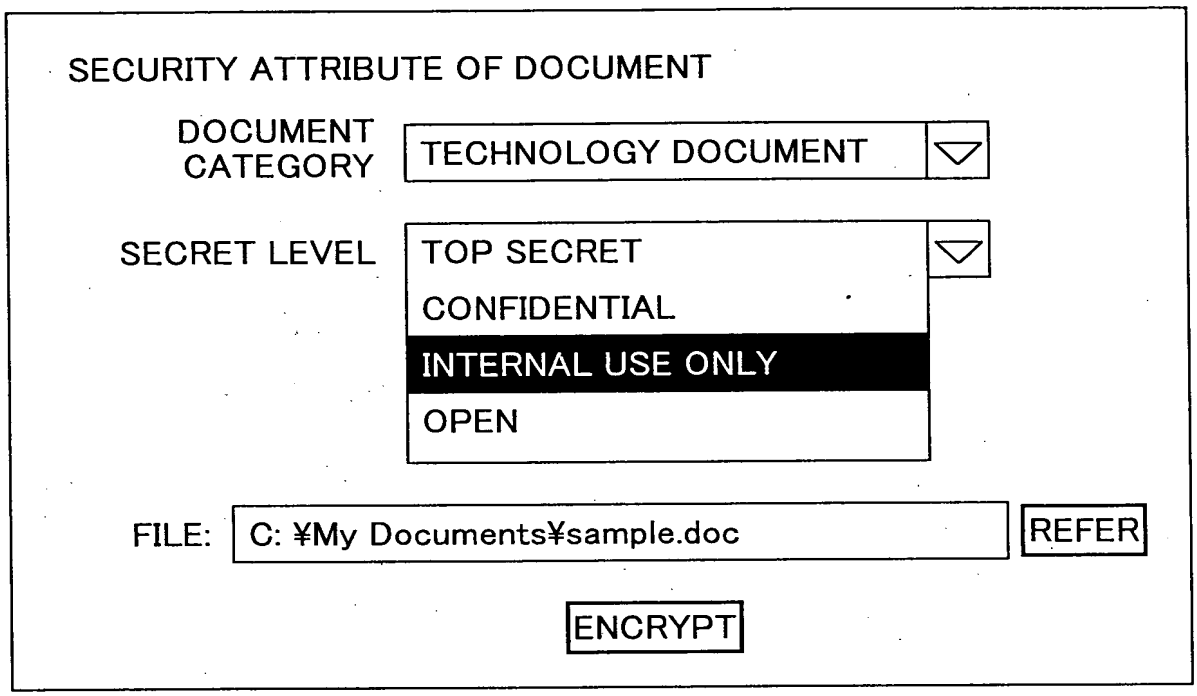
SECURITY ATTRIBUTE OF DOCUMENT
DOCUMENT CATEGORY
TECHNOLOGY DOCUMENT
SECRET LEVEL
TOP SECRET
CONFIDENTIAL
INTERNAL USE ONLY
OPEN
FILE:
C: ¥My Documents¥sample.doc
REFER
ENCRYPT

FIG.37

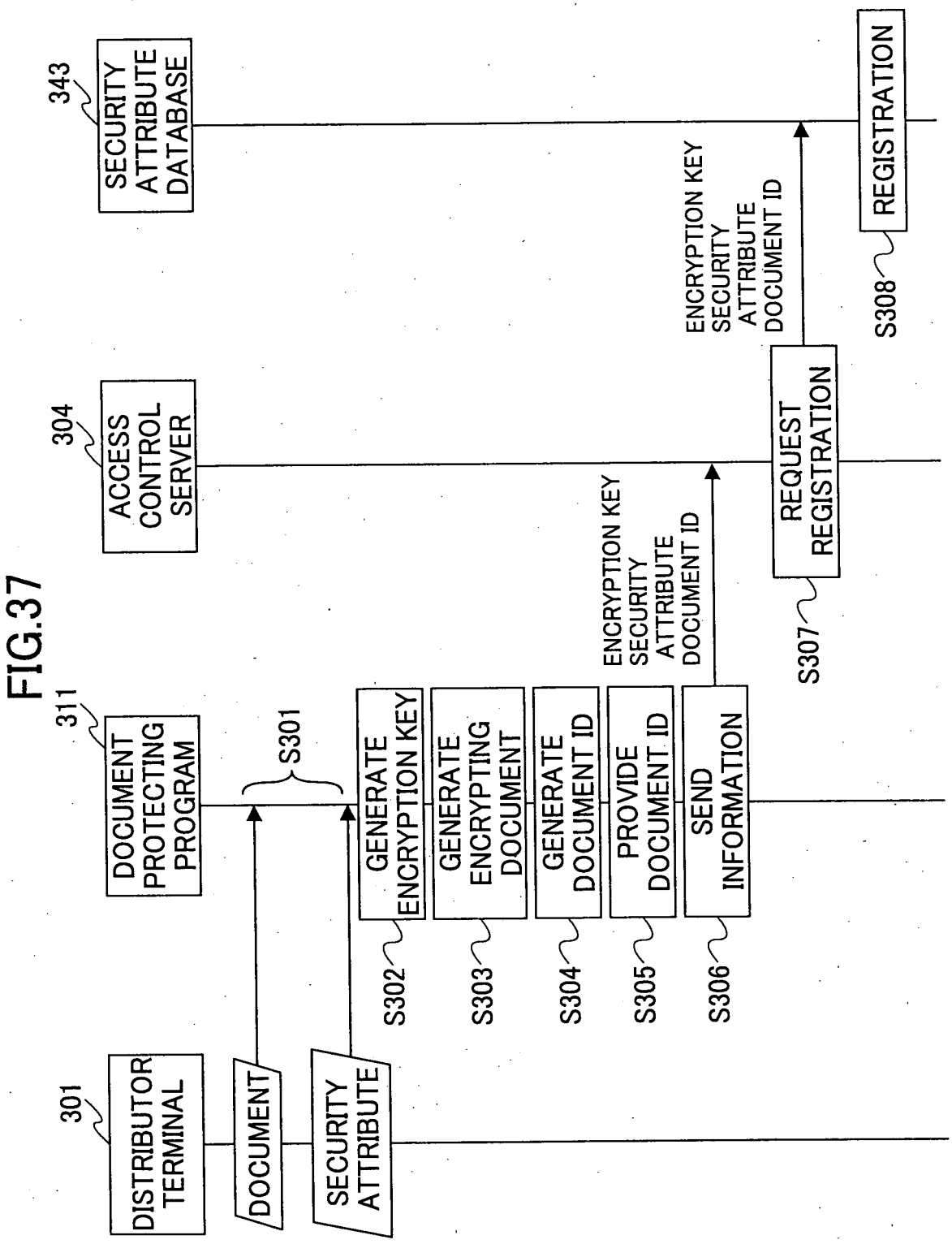
301
DISTRIBUTOR TERMINAL
DOCUMENT
SECURITY ATTRIBUTE
311
DOCUMENT PROTECTING PROGRAM
S301
GENERATE ENCRYPTION KEY
S302
GENERATE ENCRYPTING DOCUMENT
S303
GENERATE DOCUMENT ID
S304
PROVIDE DOCUMENT ID
S305
SEND INFORMATION
S306
304
ACCESS CONTROL SERVER
ENCRYPTION KEY
SECURITY ATTRIBUTE
DOCUMENT ID
REQUEST REGISTRATION
S307
343
SECURITY ATTRIBUTE DATABASE
ENCRYPTION KEY
SECURITY ATTRIBUTE
DOCUMENT ID
REGISTRATION
S308

FIG.38

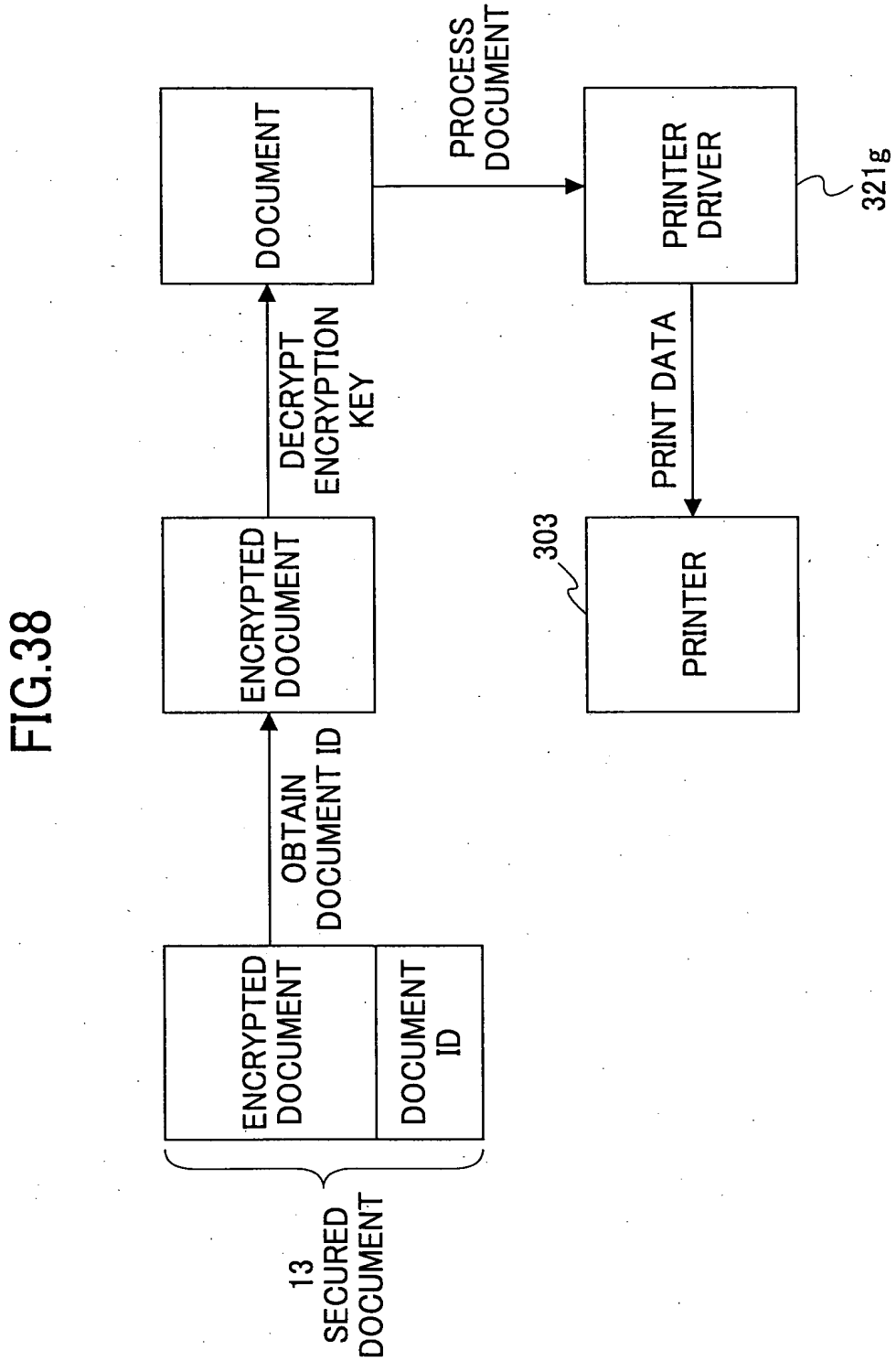
13
SECURED DOCUMENT
ENCRYPTED DOCUMENT
DOCUMENT ID
OBTAIN DOCUMENT ID
ENCRYPTED DOCUMENT
DECRYPT ENCRYPTION KEY
DOCUMENT
PROCESS DOCUMENT
PRINTER DRIVER
321g
PRINT DATA
303
PRINTER

FIG.39

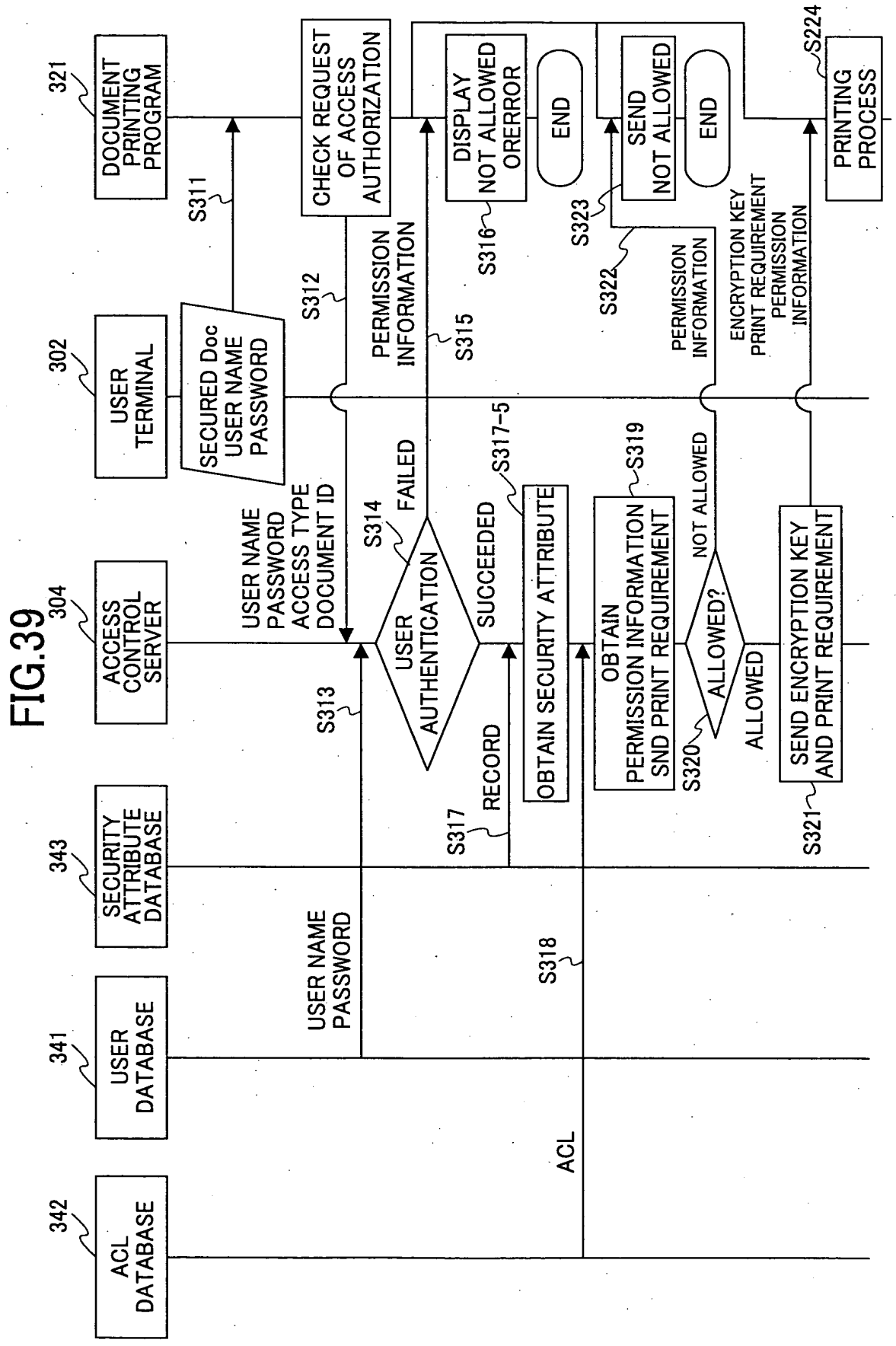
321
DOCUMENT PRINTING PROGRAM
302
USER TERMINAL
304
ACCESS CONTROL SERVER
343
SECURITY ATTRIBUTE DATABASE
341
USER DATABASE
342
ACL DATABASE
S311
SECURED Doc USER NAME PASSWORD
USER NAME PASSWORD ACCESS TYPE DOCUMENT ID
S312
CHECK REQUEST OF ACCESS AUTHORIZATION
PERMISSION INFORMATION
S315
S313
USER AUTHENTICATION
S314
FAILED
DISPLAY NOT ALLOWED ORERROR
S316
END
SUCCEEDED
S317-5
OBTAIN SECURITY ATTRIBUTE
S317
RECORD
USER NAME PASSWORD
S318
ACL
OBTAIN PERMISSION INFORMATION SND PRINT REQUIREMENT
S319
ALLOWED?
S320
NOT ALLOWED
ALLOWED
SEND ENCRYPTION KEY AND PRINT REQUIREMENT
S321
S323
SEND NOT ALLOWED
END
S322
PERMISSION INFORMATION
ENCRYPTION KEY PRINT REQUIREMENT PERMISSION INFORMATION
S224
PRINTING PROCESS

FIG.40

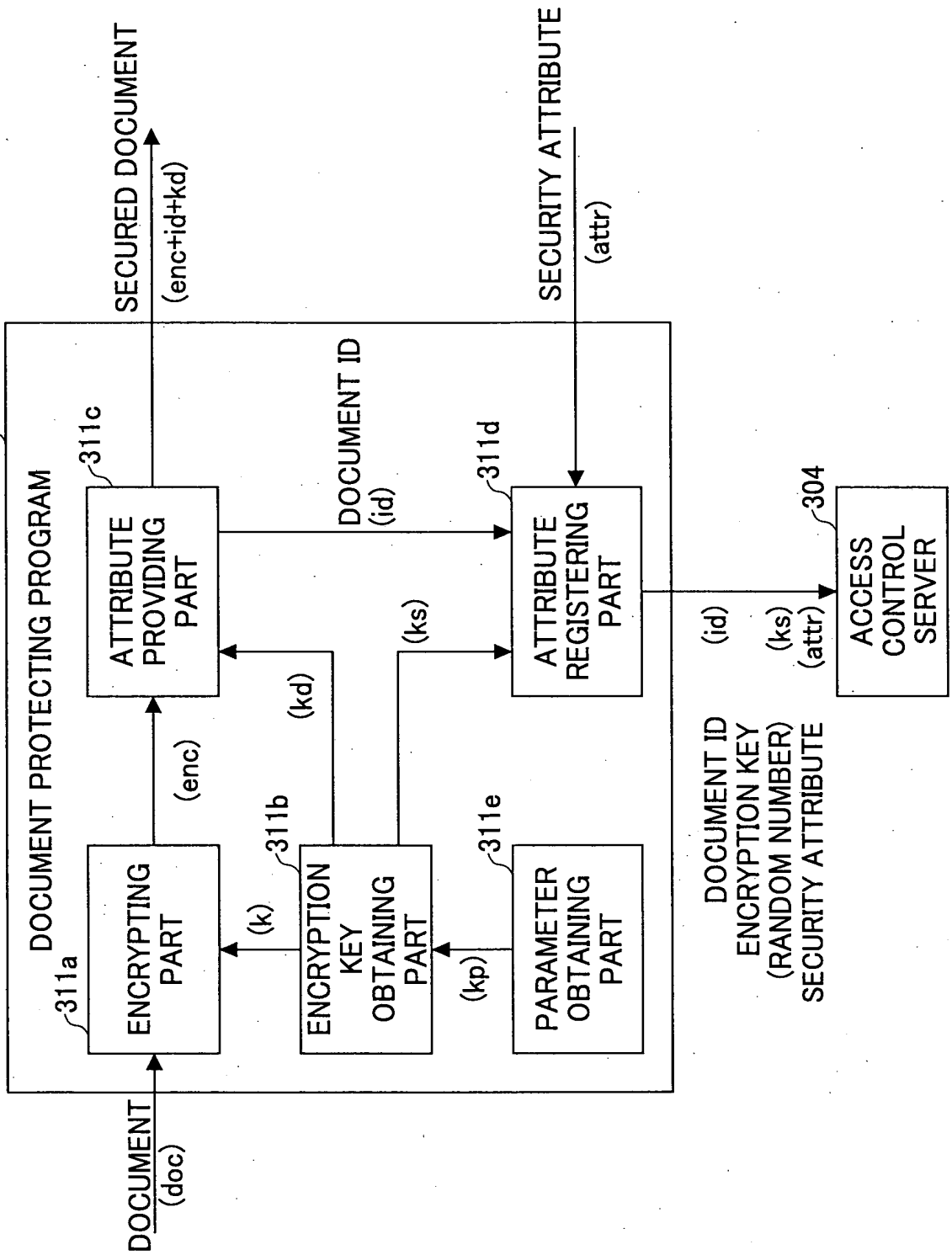
211
DOCUMENT PROTECTING PROGRAM
311a
ENCRYPTING PART
311b
ENCRYPTION KEY OBTAINING PART
311c
ATTRIBUTE PROVIDING PART
311d
ATTRIBUTE REGISTERING PART
311e
PARAMETER OBTAINING PART
DOCUMENT (doc)
SECURED DOCUMENT (enc+id+kd)
SECURITY ATTRIBUTE (attr)
DOCUMENT ID (id)
(enc)
(k)
(kd)
(kp)
(ks)
304
ACCESS CONTROL SERVER
(id)
(ks) (attr)
DOCUMENT ID
ENCRYPTION KEY (RANDOM NUMBER)
SECURITY ATTRIBUTE

FIG.41

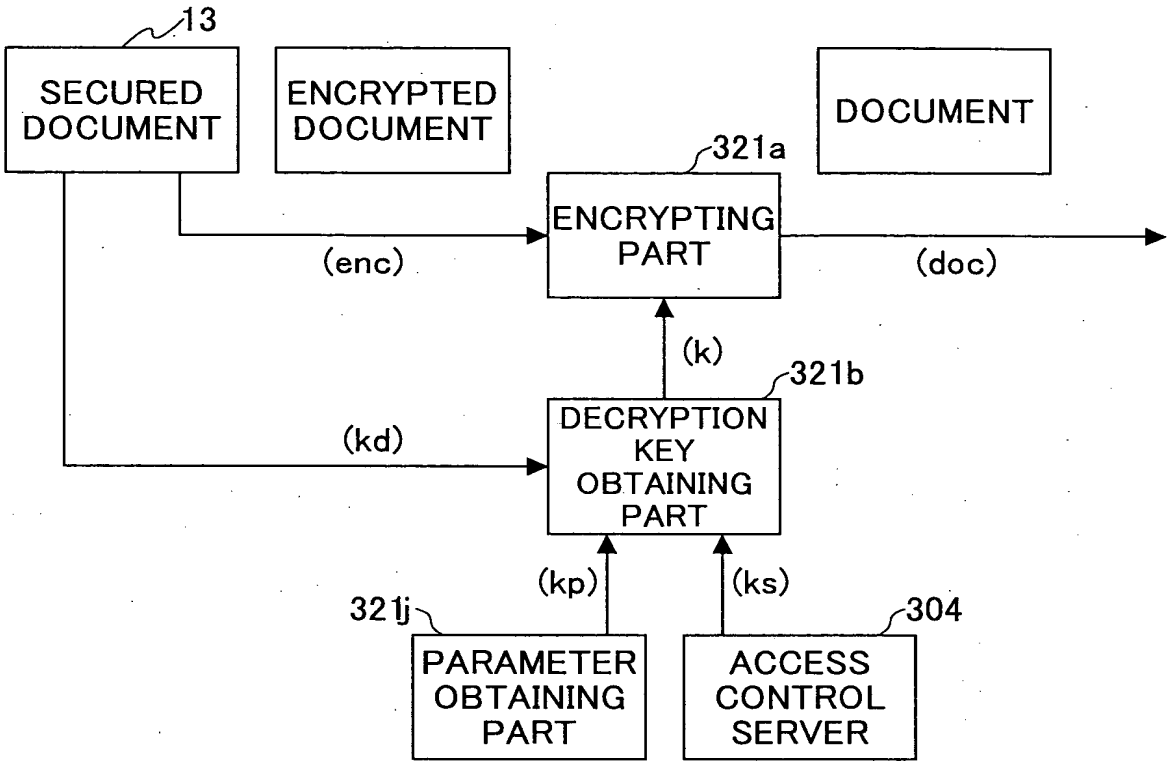
13
SECURED DOCUMENT
ENCRYPTED DOCUMENT
DOCUMENT
321a
ENCRYPTING PART
(enc)
(doc)
(k)
321b
DECRYPTION KEY OBTAINING PART
(kd)
(kp)
(ks)
321j
304
PARAMETER OBTAINING PART
ACCESS CONTROL SERVER

FIG.42

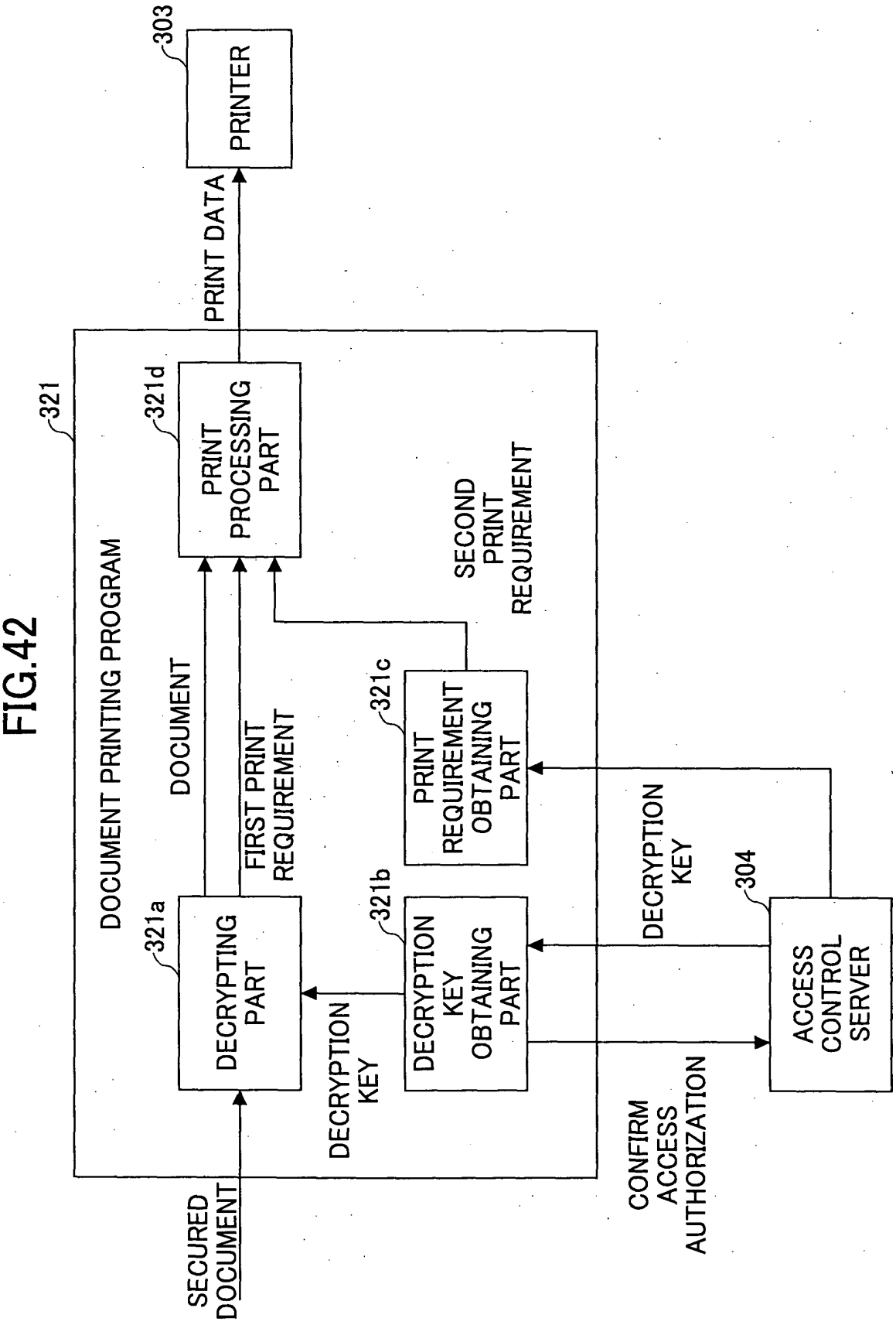
303
PRINTER
PRINT DATA
321
DOCUMENT PRINTING PROGRAM
321d
PRINT PROCESSING PART
SECOND PRINT REQUIREMENT
DOCUMENT
FIRST PRINT REQUIREMENT
321c
PRINT REQUIREMENT OBTAINING PART
321a
DECRYPTING PART
321b
DECRYPTION KEY OBTAINING PART
DECRYPTION KEY
304
ACCESS CONTROL SERVER
DECRYPTION KEY
CONFIRM ACCESS AUTHORIZATION
SECURED DOCUMENT

FIG.43

AS FOR TOP SECRET DOCUMENTS:
PROHIBIT COPYING AS A GENERAL RULE MUST BE PERMITTED BY THE MANAGEMENT REPRESENTATIVE WHEN COPY. MOREOVER, MUST RECORD THAT YOU COPIED. MUST OVERLAP WATERMARK SHOWING "PROHIBIT COPYING" WHEN PRINT. FURTHERMORE, MUST RECORD THAT YOU PRINTED.
ONLY RELATED PERSON IS ALLOWED TO READ

AS FOR CONFIDENTIAL DOCUMENTS:
ONLY RELATED PERSON IS ALLOWED TO COPY
MUST PRINT A LABEL SHOWING "CONFIDENTIAL DOCUMENT" SIMULTANEOUSLY WHEN YOU PRINTS OUT
ONLY RELATED PERSON IS ALLOWED TO READ

AS FOR INTERNAL USE ONLY DOCUMENTS:
MUST PERMITTED BY THE MANAGER WHEN YOU SENDS OUTSIDE
ALLOW TO COPY, PRINT OUT, AND READ ONLY INSIDE THE OFFICE WITHOUT PERMISSION

AS FOR PERSONNEL RELATED DOCUMENTS:
MUST HANDLE ALL AS THE CONFIDENTIAL DOCUMENT

.
.
.
.

FIG.44

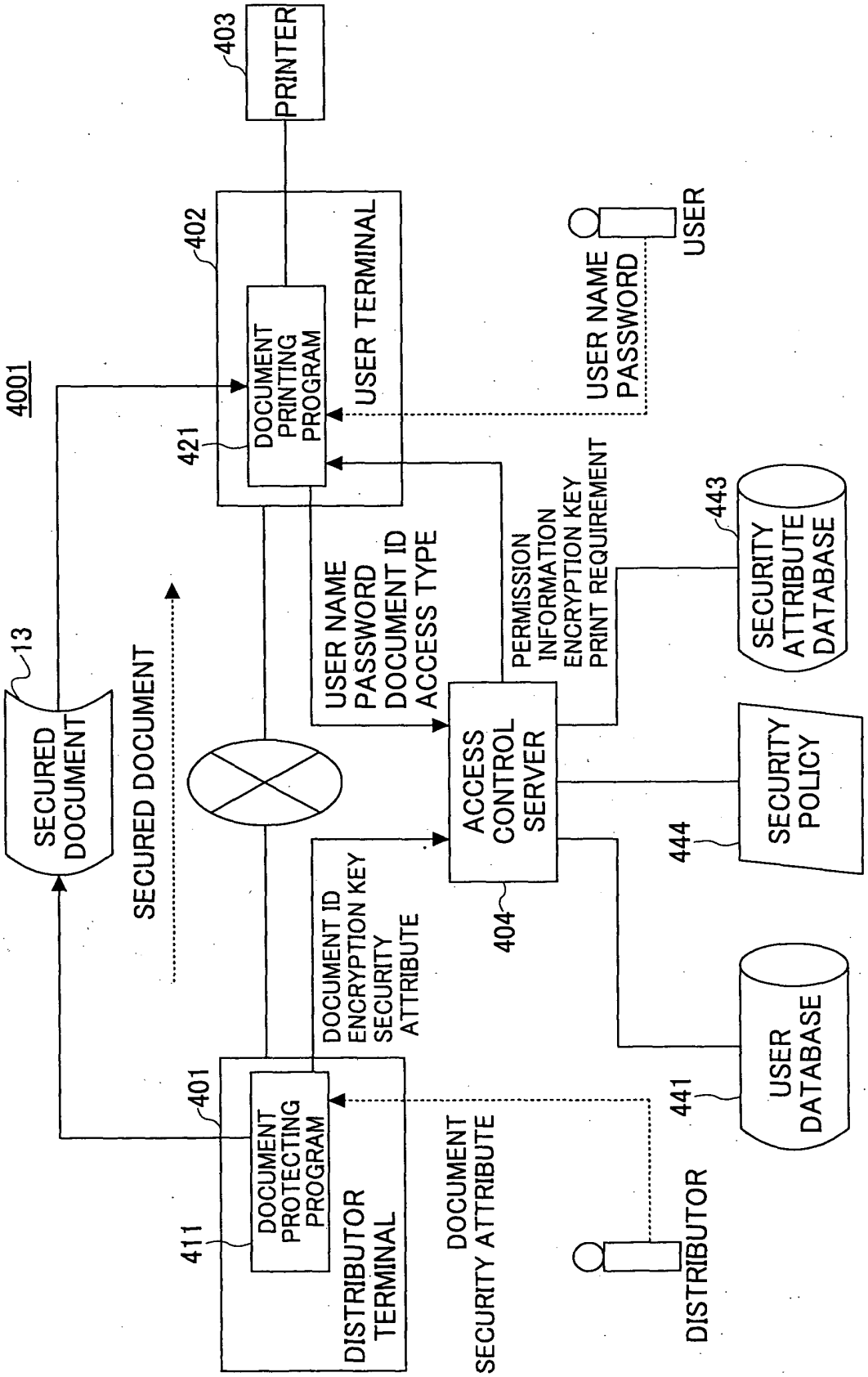
4001
403
PRINTER
402
USER TERMINAL
421
DOCUMENT PRINTING PROGRAM
USER NAME PASSWORD
USER
13
SECURED DOCUMENT
SECURED DOCUMENT
USER NAME
PASSWORD
DOCUMENT ID
ACCESS TYPE
PERMISSION INFORMATION
ENCRYPTION KEY
PRINT REQUIREMENT
443
SECURITY ATTRIBUTE DATABASE
ACCESS CONTROL SERVER
404
444
SECURITY POLICY
DOCUMENT ID
ENCRYPTION KEY
SECURITY ATTRIBUTE
401
DOCUMENT PROTECTING PROGRAM
411
DISTRIBUTOR TERMINAL
DOCUMENT SECURITY ATTRIBUTE
441
USER DATABASE
DISTRIBUTOR

FIG.45

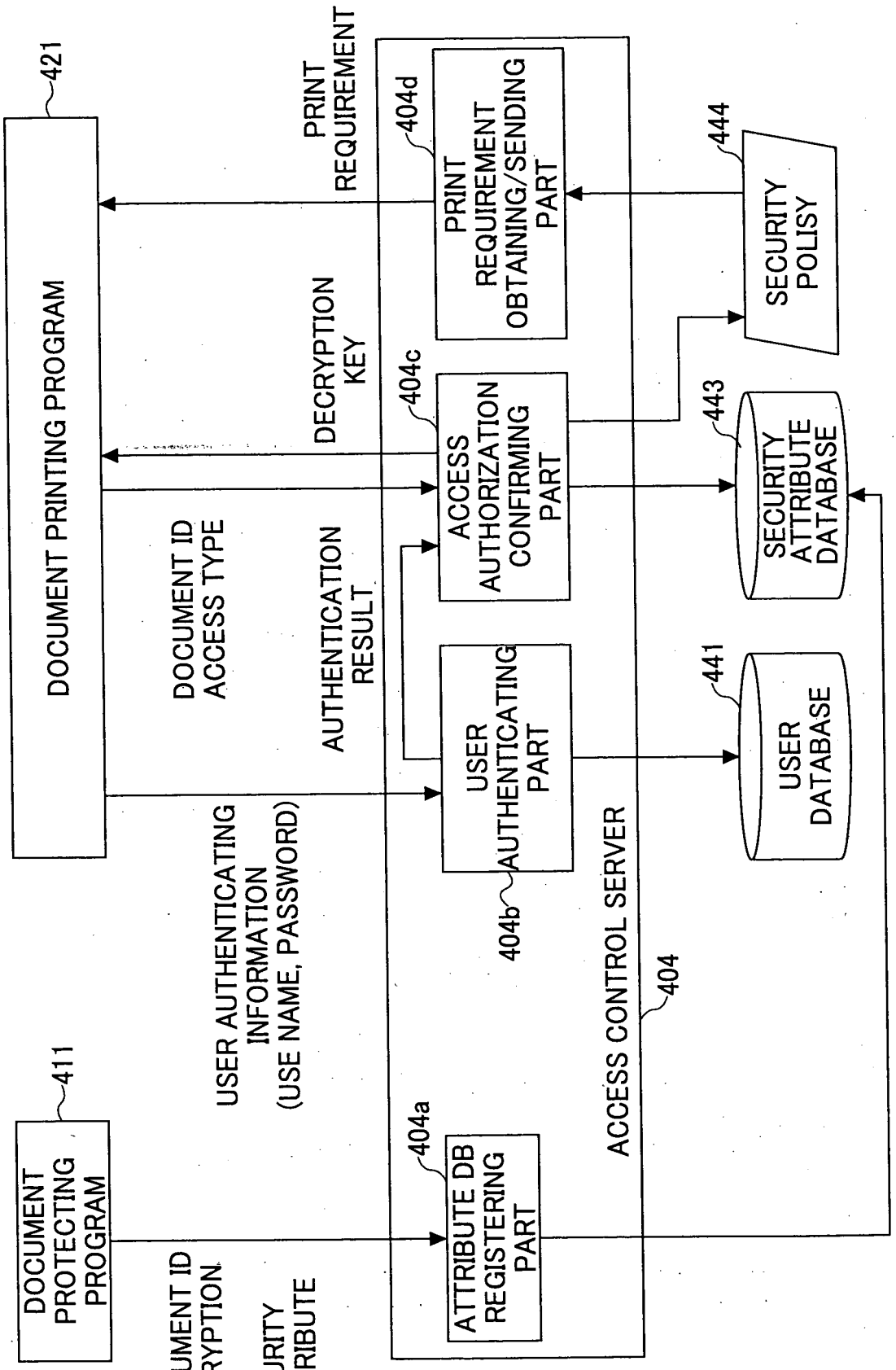
421
DOCUMENT PRINTING PROGRAM
PRINT REQUIREMENT
404d
PRINT REQUIREMENT OBTAINING/SENDING PART
444
SECURITY POLISY
DECRYPTION KEY
404c
ACCESS AUTHORIZATION CONFIRMING PART
443
SECURITY ATTRIBUTE DATABASE
DOCUMENT ID ACCESS TYPE
AUTHENTICATION RESULT
USER AUTHENTICATING INFORMATION (USE NAME, PASSWORD)
USER AUTHENTICATING PART
404b
441
USER DATABASE
ACCESS CONTROL SERVER
404
411
DOCUMENT PROTECTING PROGRAM
404a
ATTRIBUTE DB REGISTERING PART
DOCUMENT ID ENCRYPTION KEY SECURITY ATTRIBUTE

FIG.46

Document Type		User Type		Access Type	Permission	Requirement
Category	Sensitivity	Category	Level			
Technical	Secret	Technical	Medium	Read	Allowed	RAD
			High	Print	Allowed	PAC BDP EBC RAD
				Hardcopy	Denied	
				...		
Technical	Top Secret	Technical	High	...		
				...		
Human Resource	Top Secret	Human Resource	High	Read	Allowed	RAD
				Print	Denied	
				Hardcopy	Denied	

FIG.47

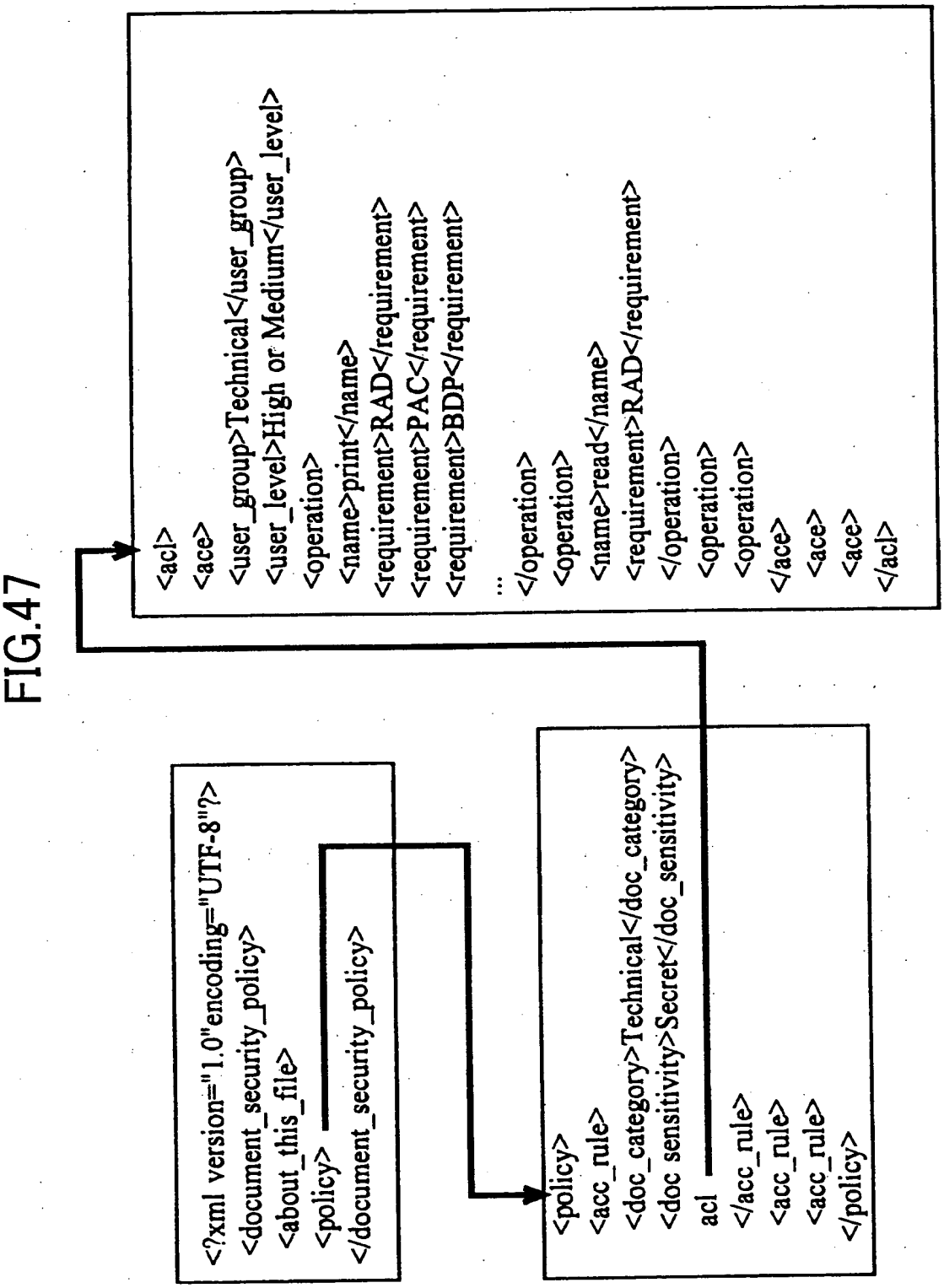
<?xml version="1.0"encoding="UTF-8"?>
<document_security_policy>
<about_this_file>
<policy>
</document_security_policy>
<policy>
<acc_rule>
<doc_category>Technical</doc_category>
<doc sensitivity>Secret</doc_sensitivity>
acl
</acc_rule>
<acc_rule>
<acc_rule>
</policy>
<acl>
<ace>
<user_group>Technical</user_group>
<user_level>High or Medium</user_level>
<operation>
<name>print</name>
<requirement>RAD</requirement>
<requirement>PAC</requirement>
<requirement>BDP</requirement>
...
</operation>
<operation>
<name>read</name>
<requirement>RAD</requirement>
</operation>
<operation>
<operation>
</ace>
<ace>
<ace>
</acl>

FIG.48

User name	Password	Category	Level
Ichiro	98q34rah	Technical	Medium
		General	Basic
Taro	Adoijoqer	Human Resource	Top Secret
		General	Basic
⋮			

FIG.49

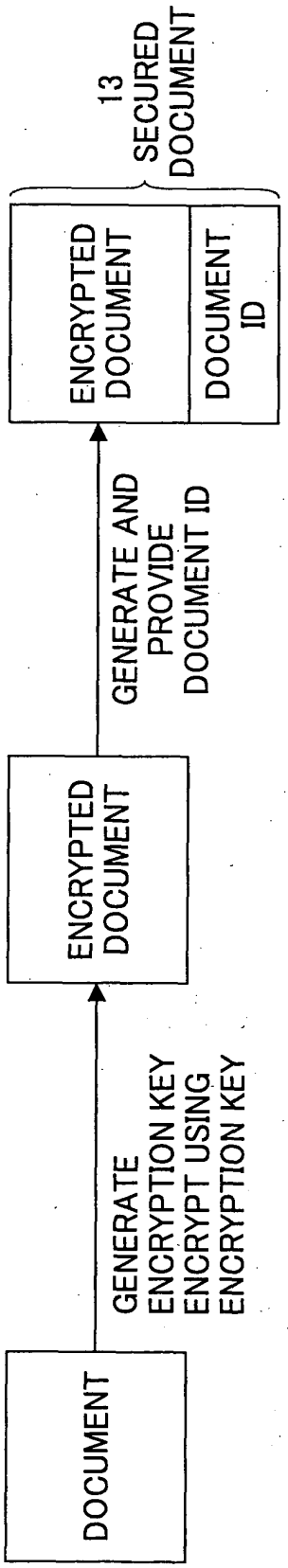
DOCUMENT
GENERATE ENCRYPTION KEY
ENCRYPT USING ENCRYPTION KEY
ENCRYPTED DOCUMENT
GENERATE AND PROVIDE DOCUMENT ID
ENCRYPTED DOCUMENT
DOCUMENT ID
13 SECURED DOCUMENT

FIG.50

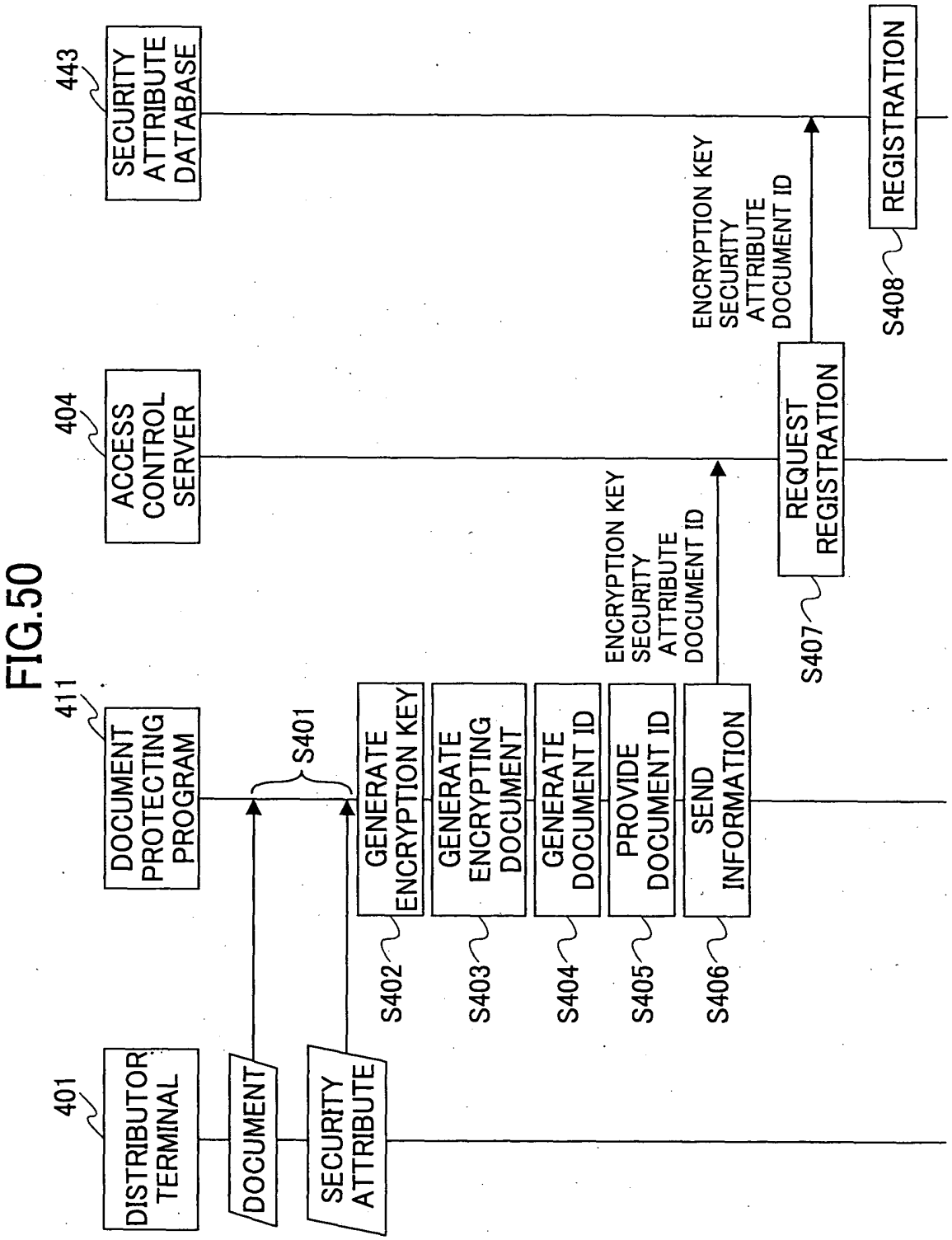
401
DISTRIBUTOR TERMINAL
411
DOCUMENT PROTECTING PROGRAM
404
ACCESS CONTROL SERVER
443
SECURITY ATTRIBUTE DATABASE
DOCUMENT
SECURITY ATTRIBUTE
S401
GENERATE ENCRYPTION KEY
GENERATE ENCRYPTING DOCUMENT
GENERATE DOCUMENT ID
PROVIDE DOCUMENT ID
SEND INFORMATION
S402
S403
S404
S405
S406
ENCRYPTION KEY
SECURITY ATTRIBUTE
DOCUMENT ID
REQUEST REGISTRATION
S407
ENCRYPTION KEY
SECURITY ATTRIBUTE
DOCUMENT ID
REGISTRATION
S408

FIG.51

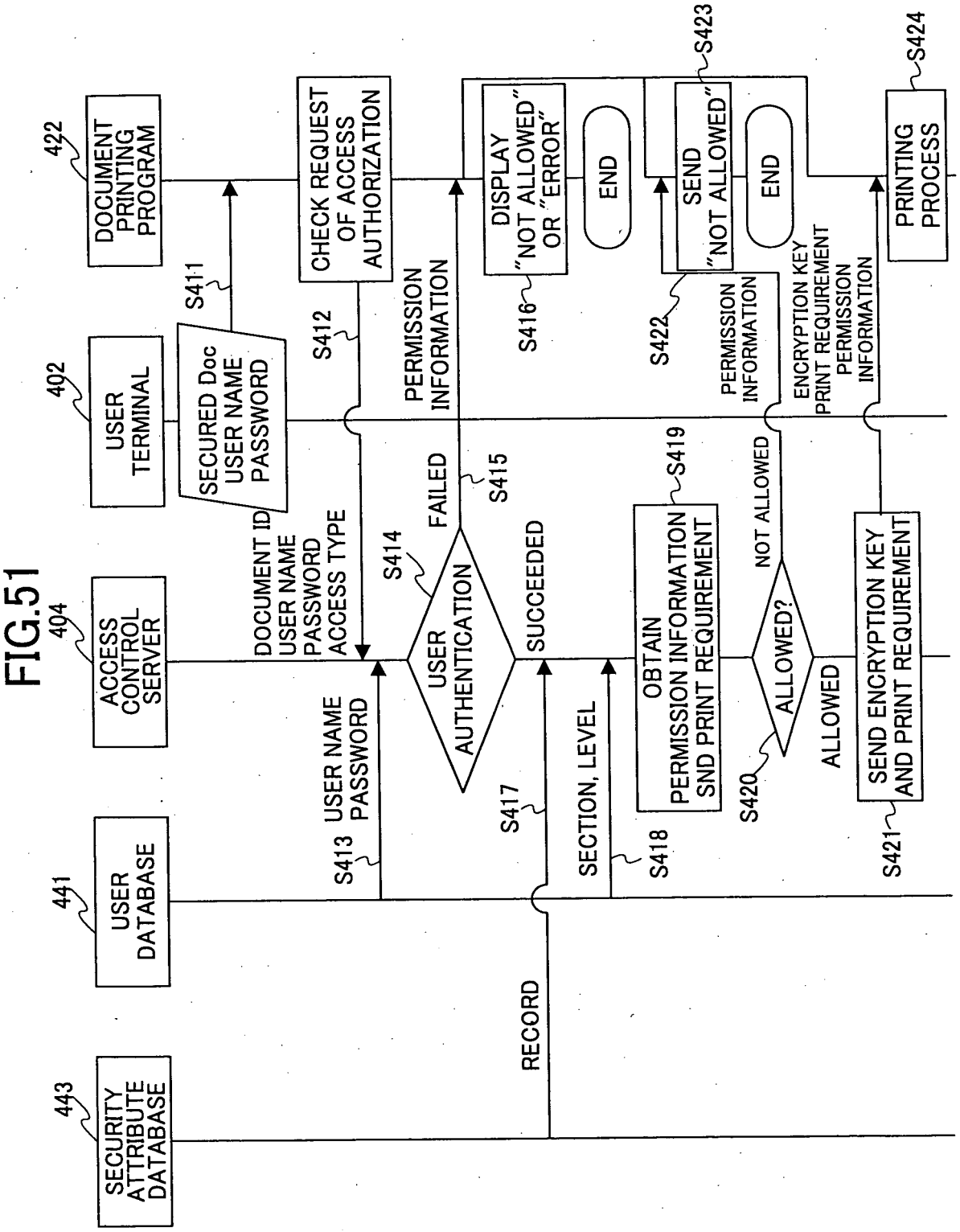
422
DOCUMENT PRINTING PROGRAM
402
USER TERMINAL
404
ACCESS CONTROL SERVER
441
USER DATABASE
443
SECURITY ATTRIBUTE DATABASE
S411
SECURED Doc USER NAME PASSWORD
DOCUMENT ID
USER NAME
PASSWORD
ACCESS TYPE
S412
CHECK REQUEST OF ACCESS AUTHORIZATION
PERMISSION INFORMATION
S413
USER NAME PASSWORD
S414
USER AUTHENTICATION
FAILED
S415
DISPLAY "NOT ALLOWED" OR "ERROR"
S416
END
SUCCEEDED
S417
SECTION, LEVEL
S418
OBTAIN PERMISSION INFORMATION SND PRINT REQUIREMENT
S419
NOT ALLOWED
ALLOWED?
S420
ALLOWED
SEND ENCRYPTION KEY AND PRINT REQUIREMENT
S421
RECORD
S422
PERMISSION INFORMATION
S423
SEND "NOT ALLOWED"
END
ENCRYPTION KEY
PRINT REQUIREMENT
PERMISSION INFORMATION
S424
PRINTING PROCESS

FIG.52

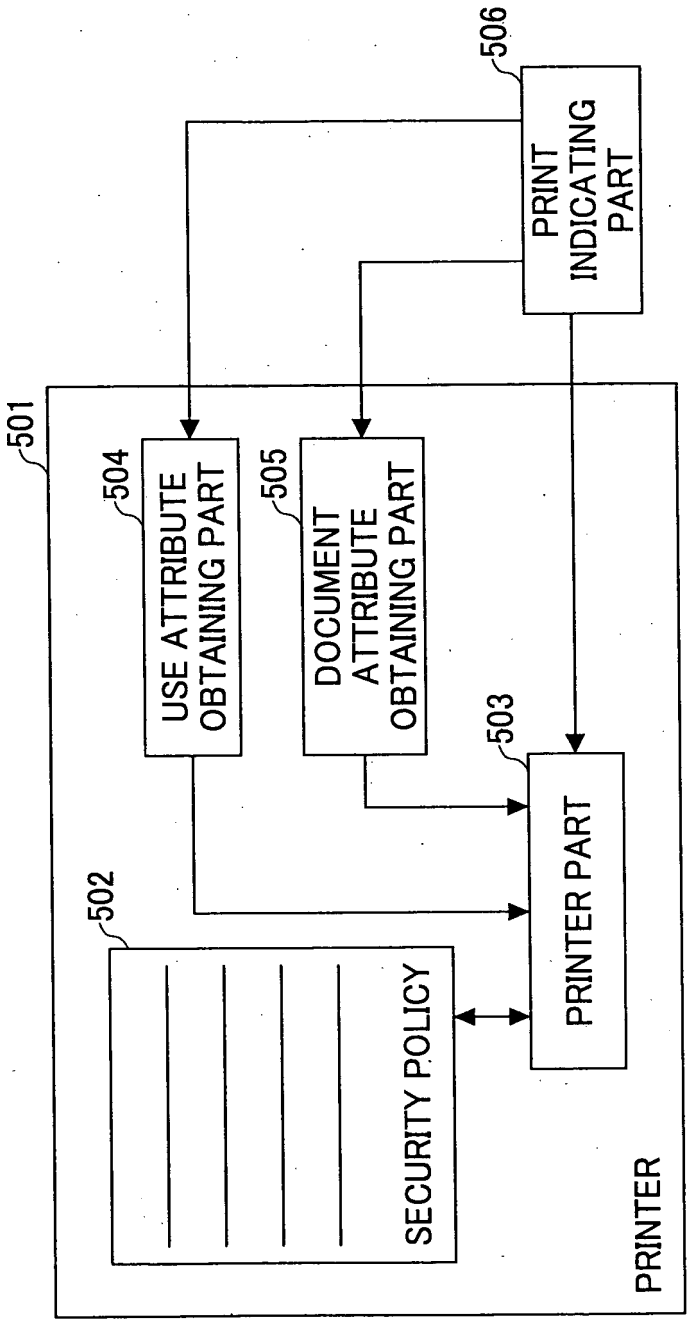
506
PRINT INDICATING PART
501
504
USE ATTRIBUTE OBTAINING PART
505
DOCUMENT ATTRIBUTE OBTAINING PART
503
PRINTER PART
502
SECURITY POLICY
PRINTER

FIG.53

502

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>basic</doc_security_level>
    <acl>
      <ace>
        <user_category>ANY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>print</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
      </ace>
    </acl>
  </acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>print</name>
          <requirement>audit</requirement>
          <requirement>embed_trace_info</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
</policy>
```

FIG.54

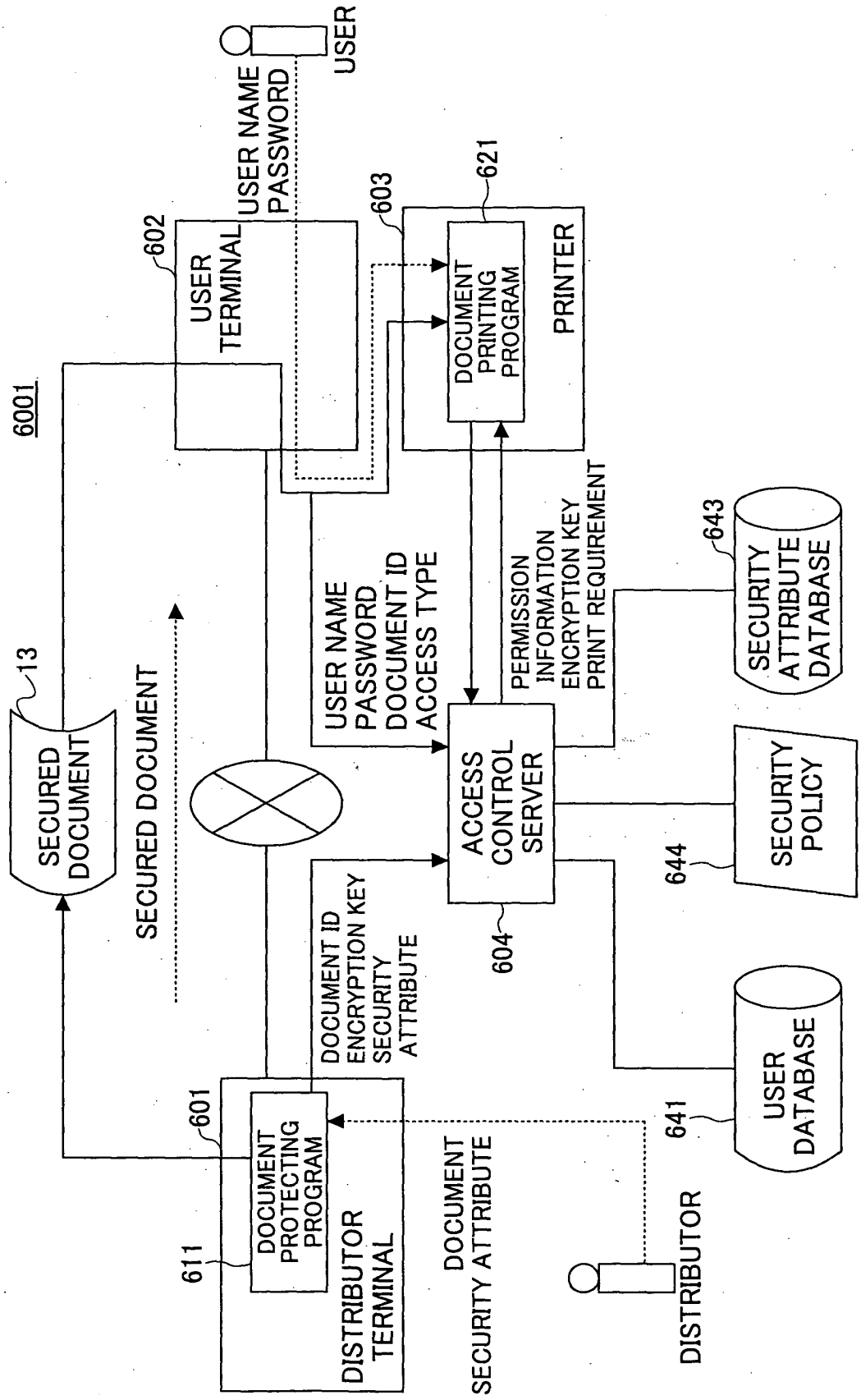
6001
USER
USER NAME
PASSWORD
602
USER TERMINAL
603
621
DOCUMENT PRINTING PROGRAM
PRINTER
13
SECURED DOCUMENT
SECURED DOCUMENT
USER NAME
PASSWORD
DOCUMENT ID
ACCESS TYPE
PERMISSION INFORMATION
ENCRYPTION KEY
PRINT REQUIREMENT
643
SECURITY ATTRIBUTE DATABASE
ACCESS CONTROL SERVER
644
SECURITY POLICY
604
DOCUMENT ID
ENCRYPTION KEY
SECURITY ATTRIBUTE
601
DOCUMENT PROTECTING PROGRAM
611
DISTRIBUTOR TERMINAL
DOCUMENT SECURITY ATTRIBUTE
641
USER DATABASE
DISTRIBUTOR

FIG.55

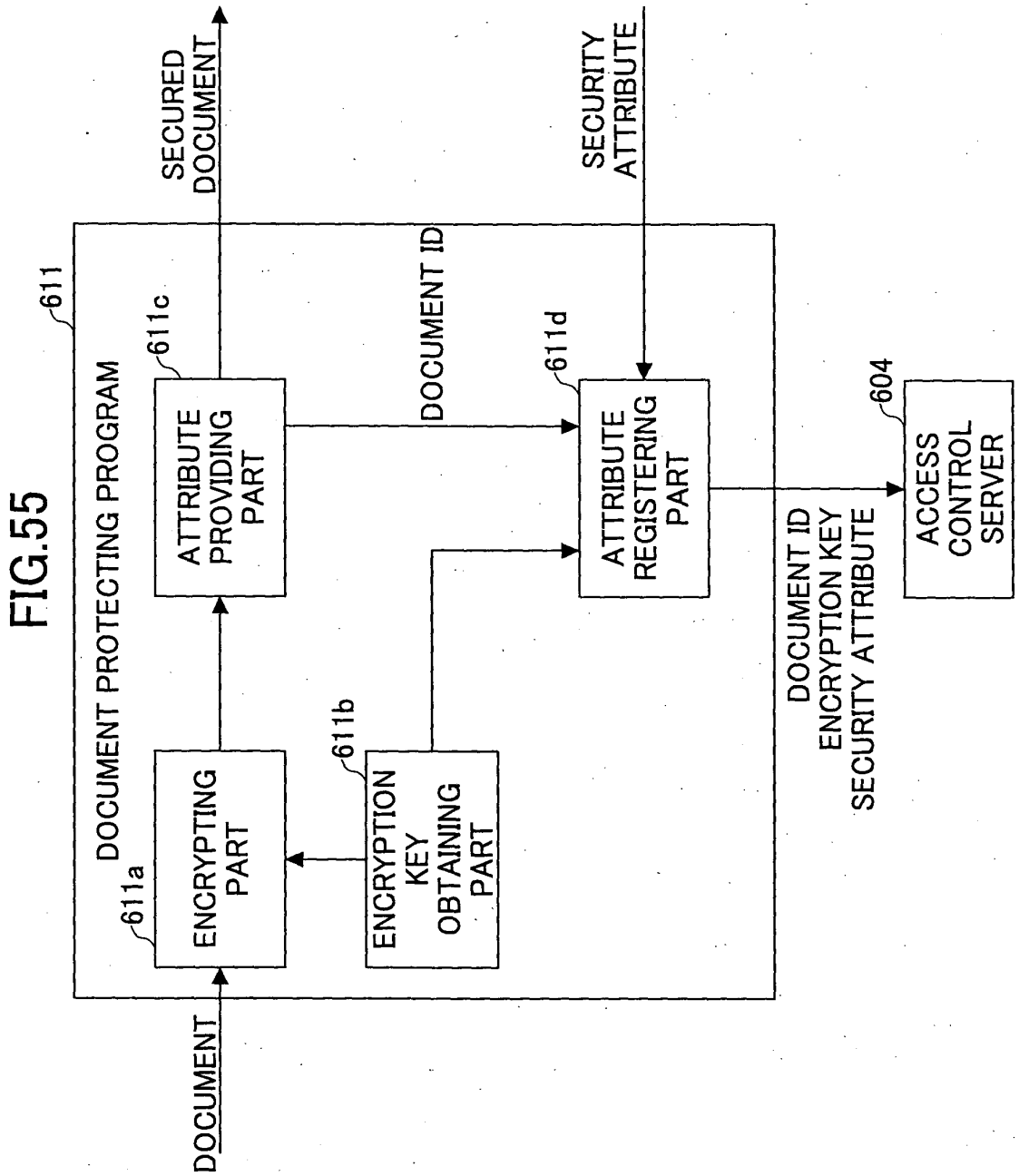
DOCUMENT
SECURED DOCUMENT
SECURITY ATTRIBUTE
611
DOCUMENT PROTECTING PROGRAM
611a
ENCRYPTING PART
611b
ENCRYPTION KEY OBTAINING PART
611c
ATTRIBUTE PROVIDING PART
611d
ATTRIBUTE REGISTERING PART
DOCUMENT ID
DOCUMENT ID
ENCRYPTION KEY
SECURITY ATTRIBUTE
604
ACCESS CONTROL SERVER

FIG.56

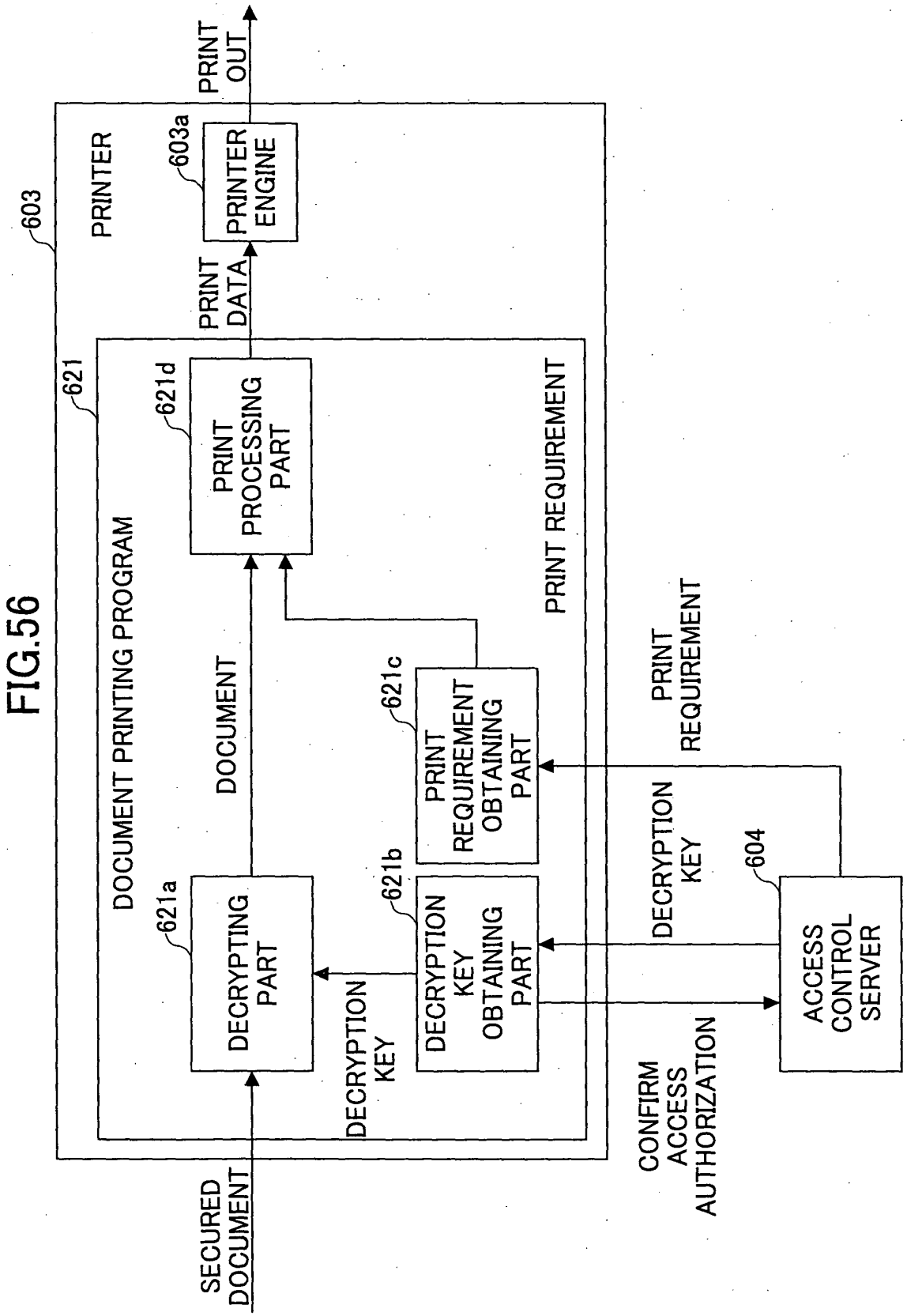
603
PRINTER
603a
PRINTER ENGINE
PRINT OUT
PRINT DATA
621
DOCUMENT PRINTING PROGRAM
621d
PRINT PROCESSING PART
PRINT REQUIREMENT
DOCUMENT
621c
PRINT REQUIREMENT OBTAINING PART
PRINT REQUIREMENT
621a
DECRYPTING PART
621b
DECRYPTION KEY OBTAINING PART
DECRYPTION KEY
604
ACCESS CONTROL SERVER
DECRYPTION KEY
CONFIRM ACCESS AUTHORIZATION
SECURED DOCUMENT

FIG.57

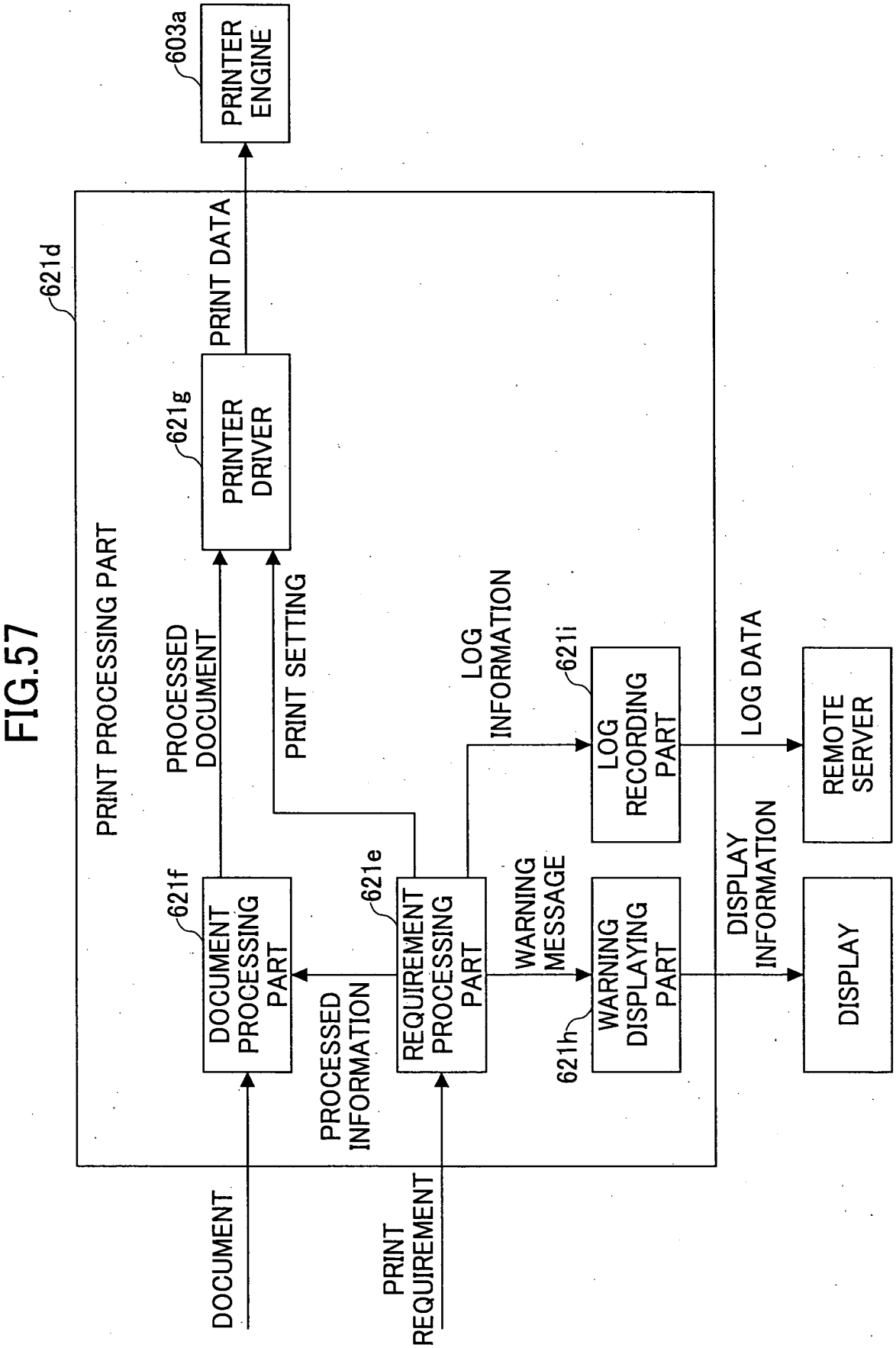
603a
PRINTER ENGINE
621d
PRINT PROCESSING PART
PRINT DATA
621g
PRINTER DRIVER
PROCESSED DOCUMENT
PRINT SETTING
LOG INFORMATION
621i
LOG RECORDING PART
LOG DATA
REMOTE SERVER
621f
DOCUMENT PROCESSING PART
621e
REQUIREMENT PROCESSING PART
WARNING MESSAGE
621h
WARNING DISPLAYING PART
DISPLAY INFORMATION
DISPLAY
PROCESSED INFORMATION
DOCUMENT
PRINT REQUIREMENT

FIG.58

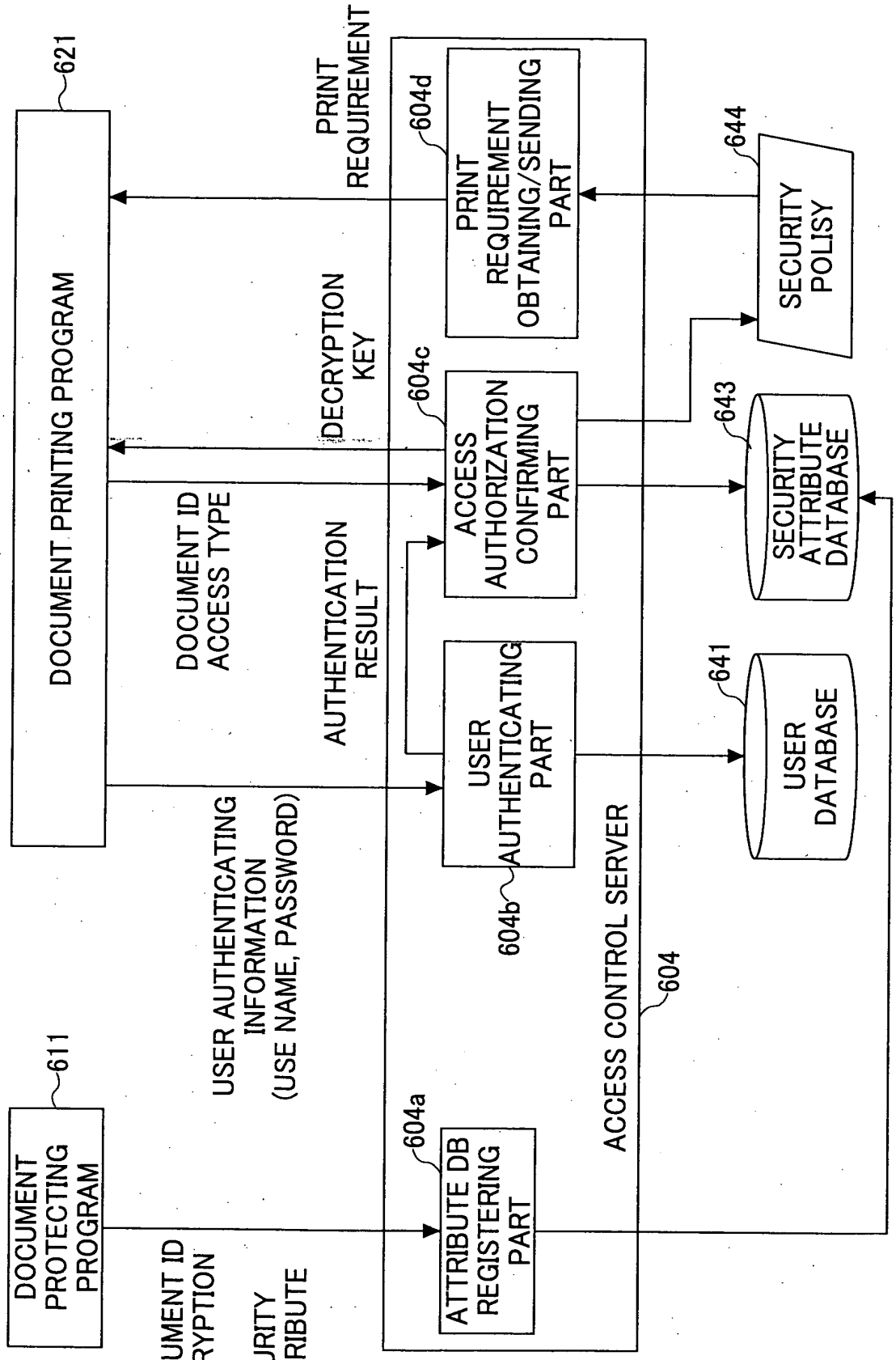
DOCUMENT PROTECTING PROGRAM
611
DOCUMENT ID
ENCRYPTION KEY
SECURITY ATTRIBUTE
DOCUMENT PRINTING PROGRAM
621
USER AUTHENTICATING INFORMATION (USE NAME, PASSWORD)
DOCUMENT ID ACCESS TYPE
AUTHENTICATION RESULT
DECRYPTION KEY
PRINT REQUIREMENT
ACCESS CONTROL SERVER
604
ATTRIBUTE DB REGISTERING PART
604a
USER AUTHENTICATING PART
604b
ACCESS AUTHORIZATION CONFIRMING PART
604c
PRINT REQUIREMENT OBTAINING/SENDING PART
604d
USER DATABASE
641
SECURITY ATTRIBUTE DATABASE
643
SECURITY POLISY
644

FIG.59

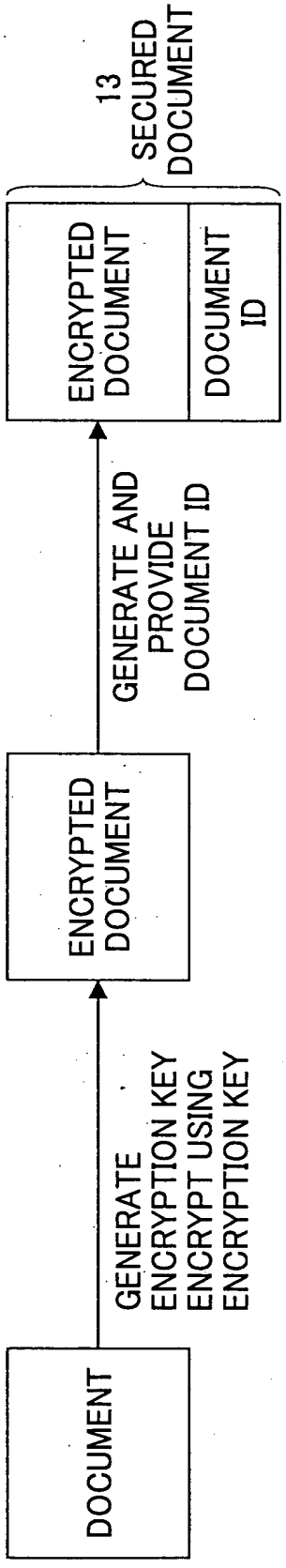
DOCUMENT
GENERATE ENCRYPTION KEY
ENCRYPT USING ENCRYPTION KEY
ENCRYPTED DOCUMENT
GENERATE AND PROVIDE DOCUMENT ID
ENCRYPTED DOCUMENT
DOCUMENT ID
13 SECURED DOCUMENT

FIG.60

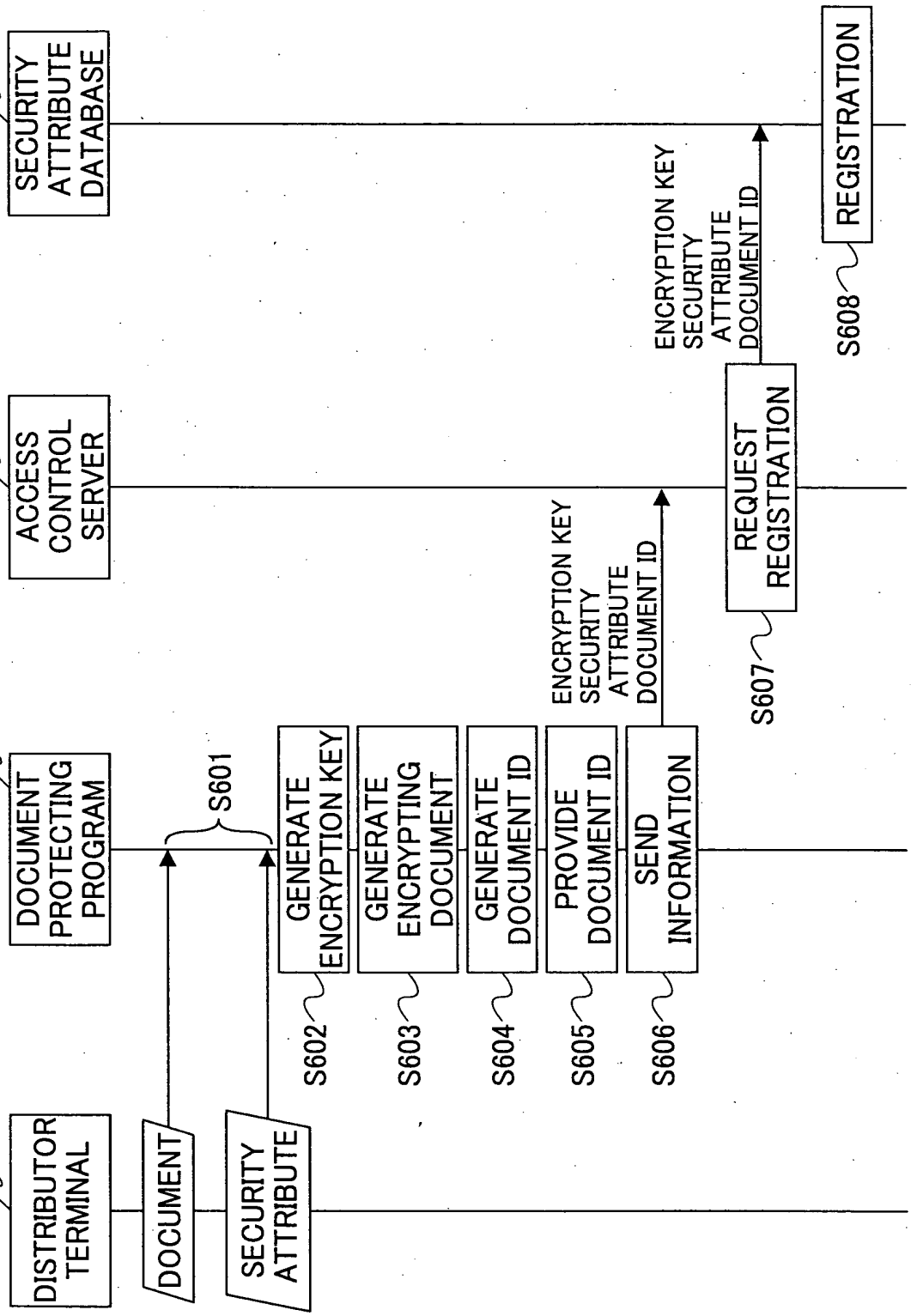
601
DISTRIBUTOR TERMINAL
DOCUMENT
SECURITY ATTRIBUTE
611
DOCUMENT PROTECTING PROGRAM
S601
GENERATE ENCRYPTION KEY
S602
GENERATE ENCRYPTING DOCUMENT
S603
GENERATE DOCUMENT ID
S604
PROVIDE DOCUMENT ID
S605
SEND INFORMATION
S606
604
ACCESS CONTROL SERVER
ENCRYPTION KEY
SECURITY ATTRIBUTE
DOCUMENT ID
REQUEST REGISTRATION
S607
643
SECURITY ATTRIBUTE DATABASE
ENCRYPTION KEY
SECURITY ATTRIBUTE
DOCUMENT ID
REGISTRATION
S608

FIG.61

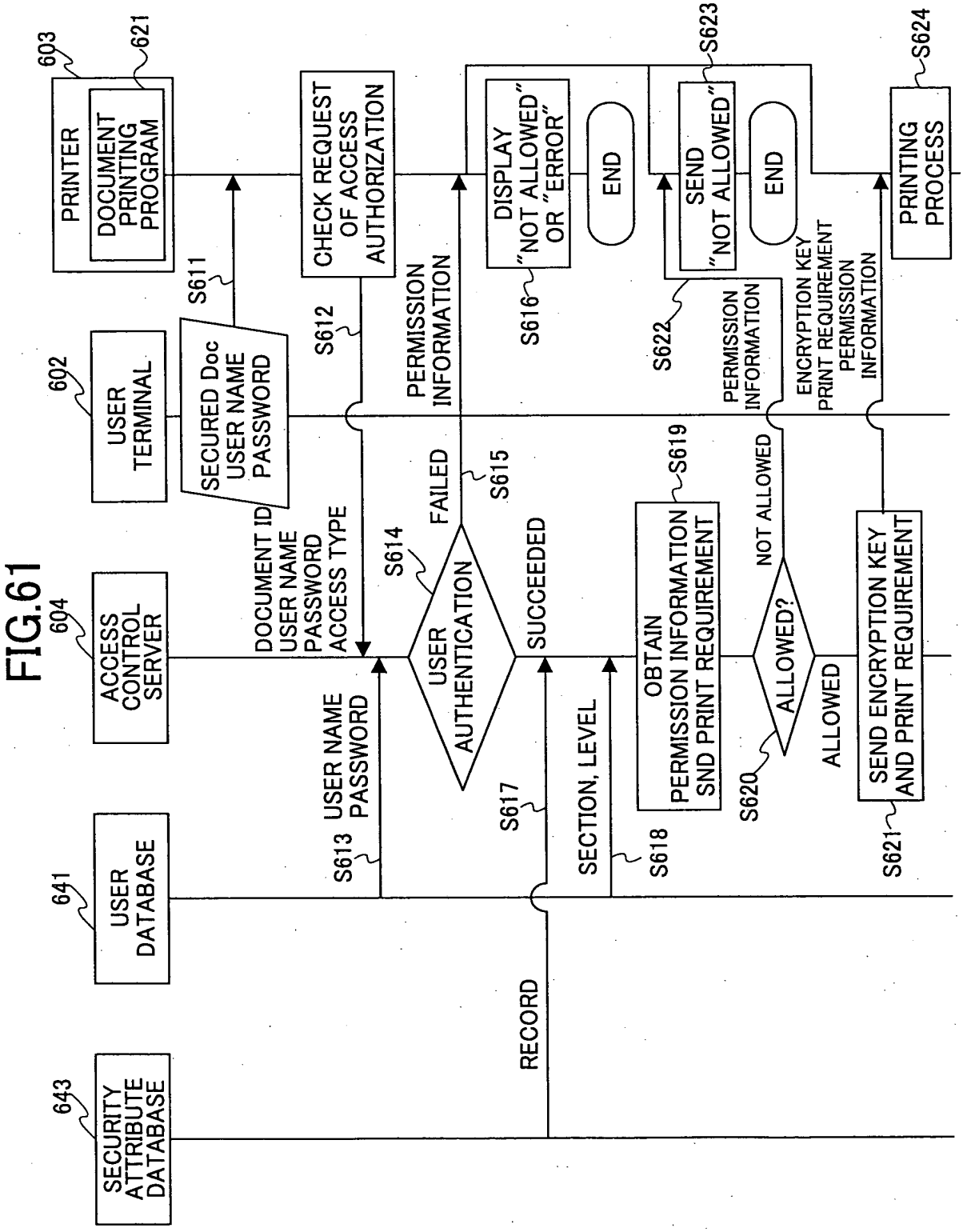
PRINTER
DOCUMENT PRINTING PROGRAM
603
621
USER TERMINAL
602
SECURED Doc USER NAME PASSWORD
S611
CHECK REQUEST OF ACCESS AUTHORIZATION
S612
PERMISSION INFORMATION
DISPLAY "NOT ALLOWED" OR "ERROR"
S616
END
SEND "NOT ALLOWED"
S623
END
S622
PERMISSION INFORMATION
ENCRYPTION KEY PRINT REQUIREMENT PERMISSION INFORMATION
PRINTING PROCESS
S624
ACCESS CONTROL SERVER
604
DOCUMENT ID
USER NAME
PASSWORD
ACCESS TYPE
S614
USER AUTHENTICATION
FAILED
S615
SUCCEEDED
OBTAIN PERMISSION INFORMATION SND PRINT REQUIREMENT
S619
NOT ALLOWED
ALLOWED?
S620
ALLOWED
SEND ENCRYPTION KEY AND PRINT REQUIREMENT
S621
USER DATABASE
641
USER NAME
PASSWORD
S613
S617
SECTION, LEVEL
S618
RECORD
SECURITY ATTRIBUTE DATABASE
643

FIG.62

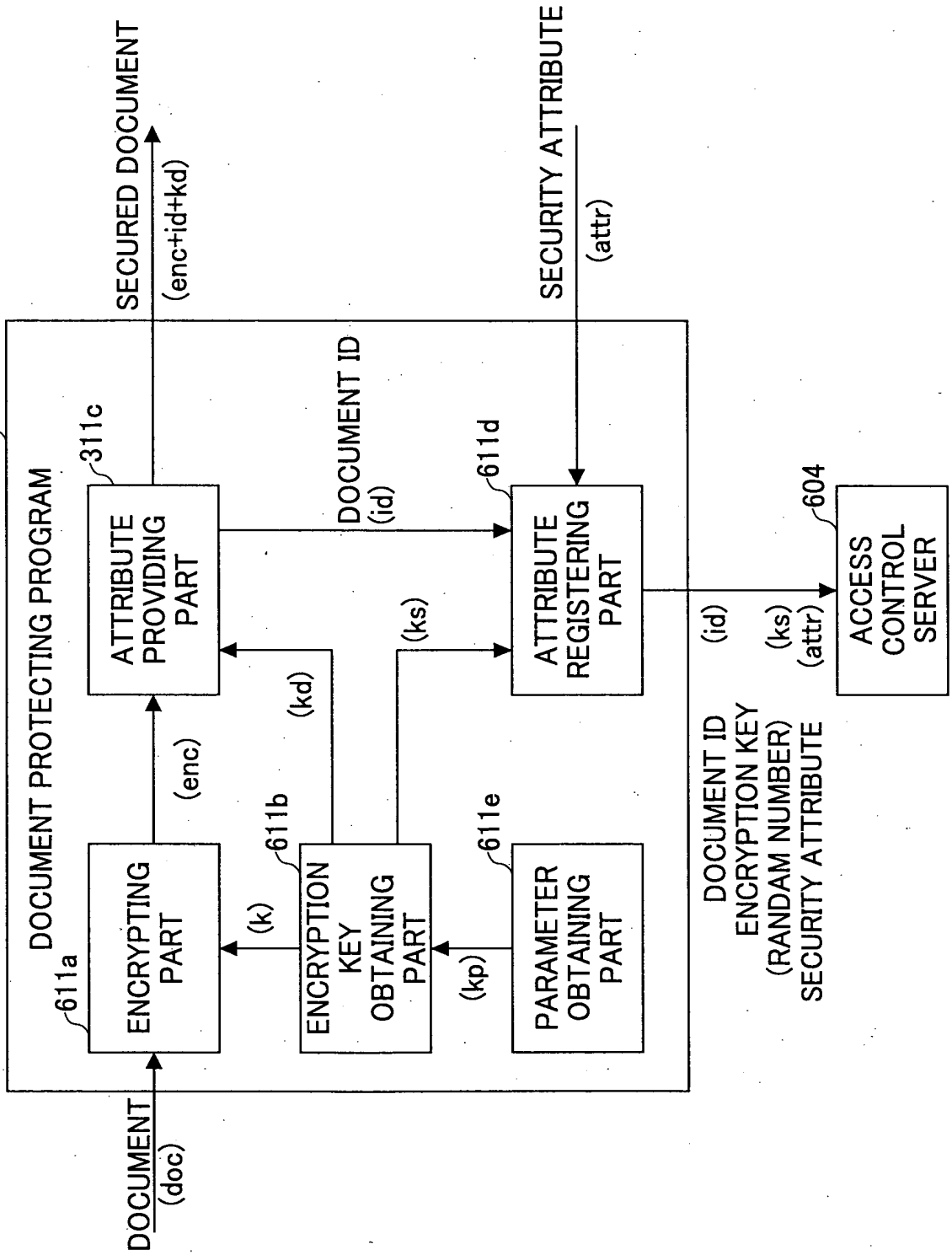
611
DOCUMENT PROTECTING PROGRAM
611a
ENCRYPTING PART
611b
ENCRYPTION KEY OBTAINING PART
611e
PARAMETER OBTAINING PART
311c
ATTRIBUTE PROVIDING PART
611d
ATTRIBUTE REGISTERING PART
604
ACCESS CONTROL SERVER
DOCUMENT
(doc)
(enc)
(k)
(kp)
(kd)
(ks)
SECURED DOCUMENT
(enc+id+kd)
DOCUMENT ID
(id)
SECURITY ATTRIBUTE
(attr)
(id)
(ks)
(attr)
DOCUMENT ID
ENCRYPTION KEY
(RANDAM NUMBER)
SECURITY ATTRIBUTE

FIG.63

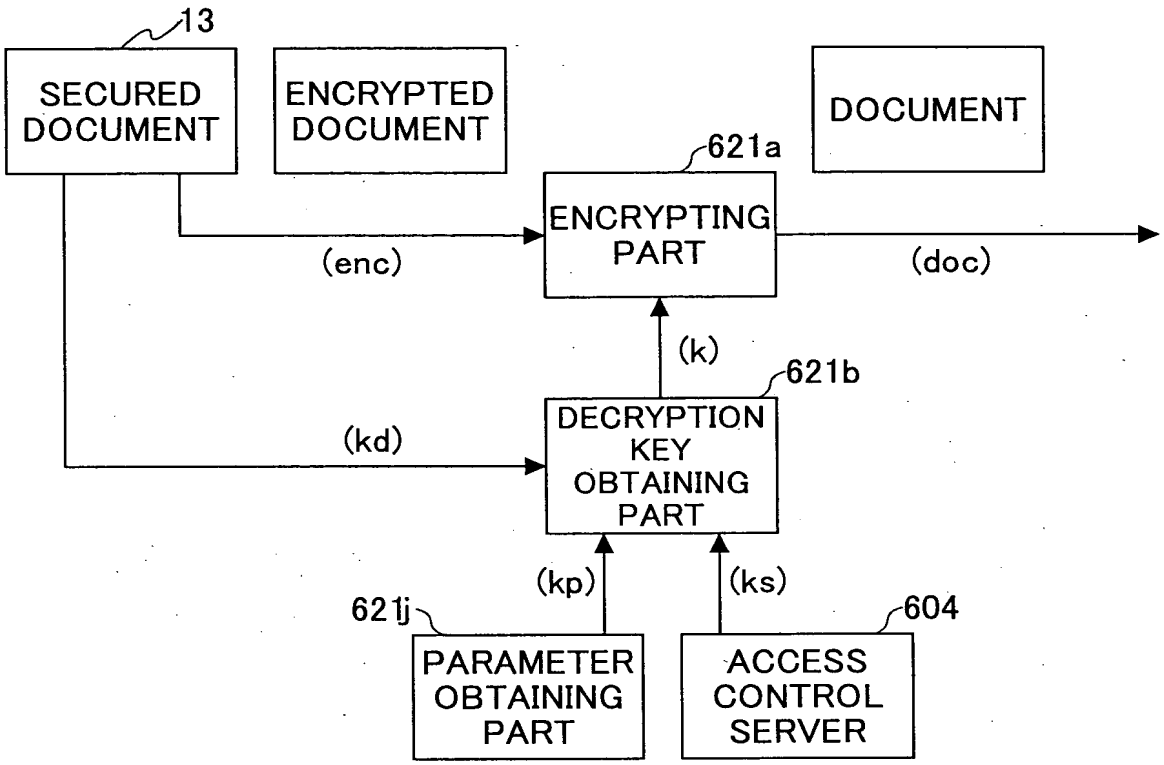
13
SECURED DOCUMENT
ENCRYPTED DOCUMENT
DOCUMENT
621a
ENCRYPTING PART
(enc)
(doc)
(k)
621b
DECRYPTION KEY OBTAINING PART
(kd)
(kp)
(ks)
621j
PARAMETER OBTAINING PART
604
ACCESS CONTROL SERVER

FIG.64

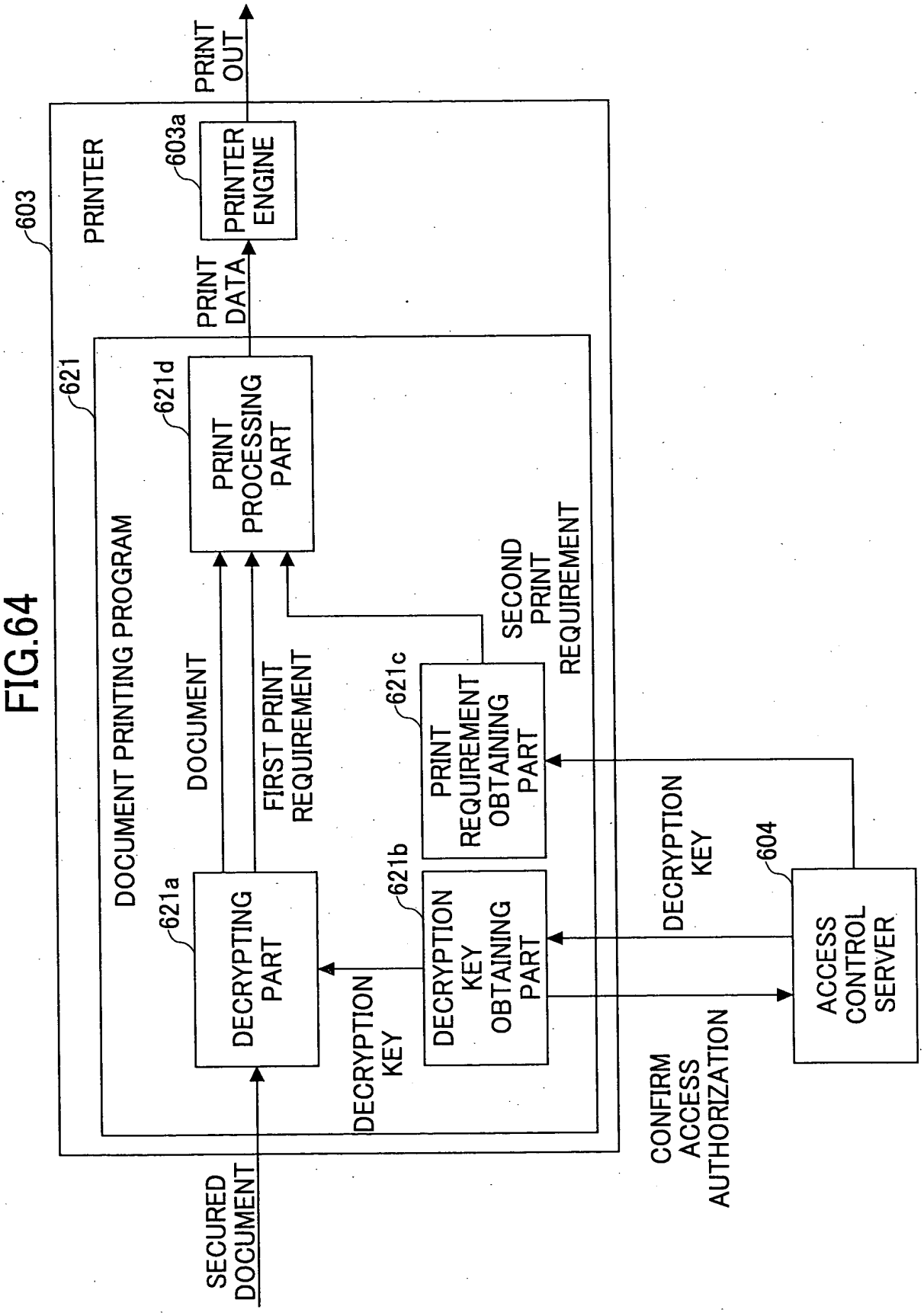
603
PRINTER
603a
PRINTER ENGINE
PRINT OUT
PRINT DATA
621
DOCUMENT PRINTING PROGRAM
621d
PRINT PROCESSING PART
DOCUMENT
FIRST PRINT REQUIREMENT
SECOND PRINT REQUIREMENT
621c
PRINT REQUIREMENT OBTAINING PART
621a
DECRYPTING PART
621b
DECRYPTION KEY OBTAINING PART
DECRYPTION KEY
DECRYPTION KEY
604
ACCESS CONTROL SERVER
CONFIRM ACCESS AUTHORIZATION
SECURED DOCUMENT

FIG.65

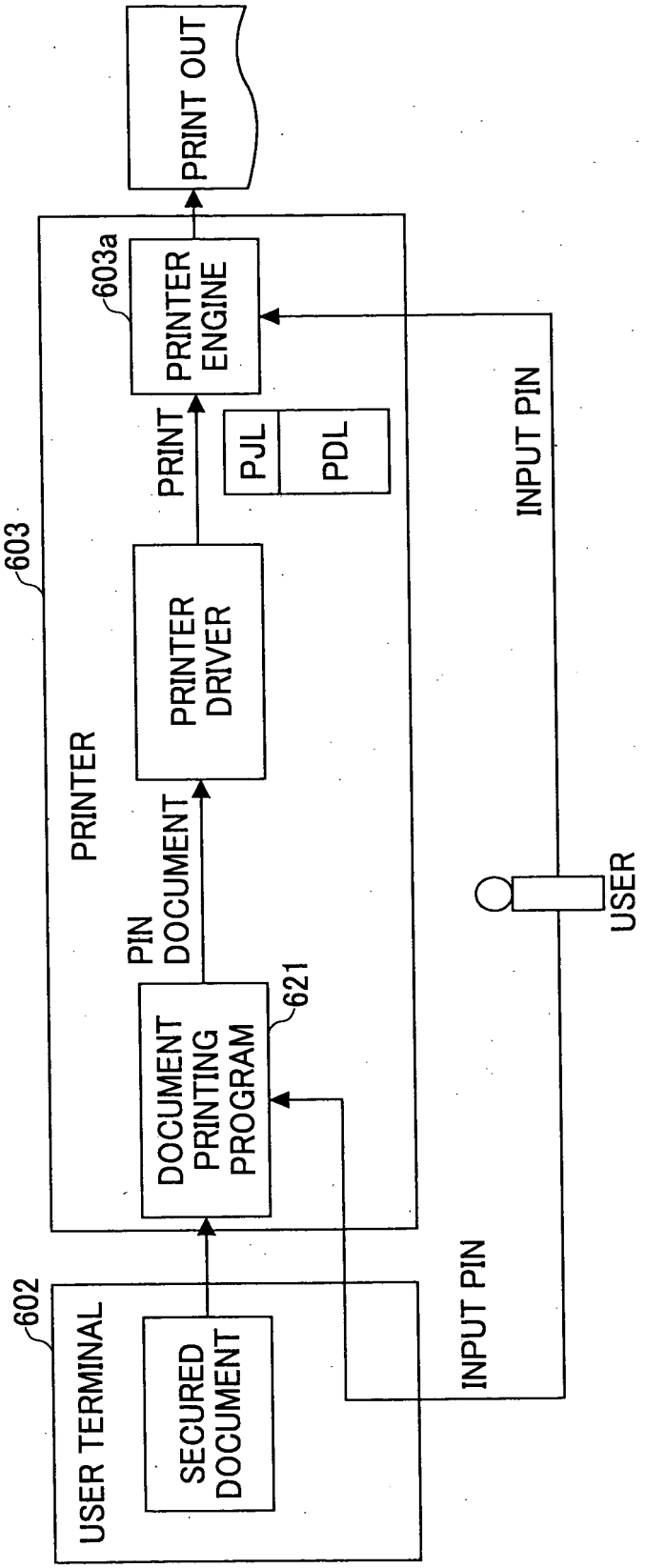
PRINT OUT
603a
PRINTER ENGINE
PRINT
PJL
PDL
603
PRINTER
PRINTER DRIVER
PIN DOCUMENT
621
DOCUMENT PRINTING PROGRAM
INPUT PIN
USER
602
USER TERMINAL
SECURED DOCUMENT
INPUT PIN

FIG.66A

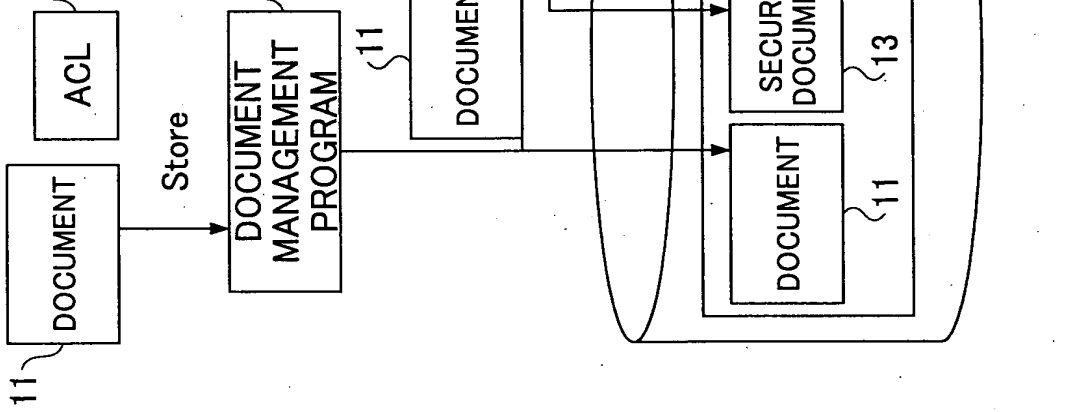

FIG.66B

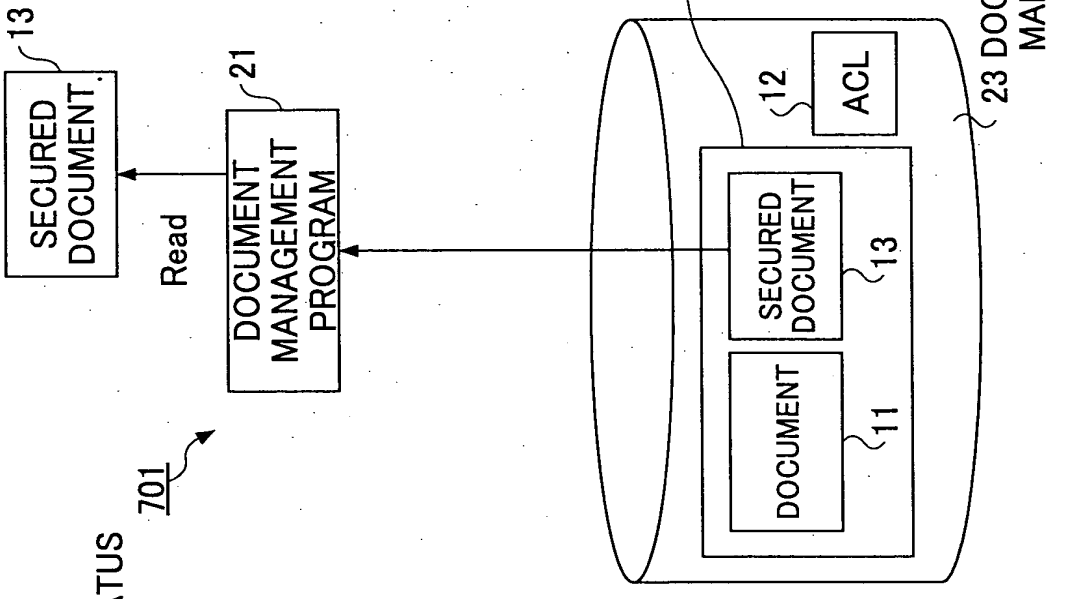

FIG.67

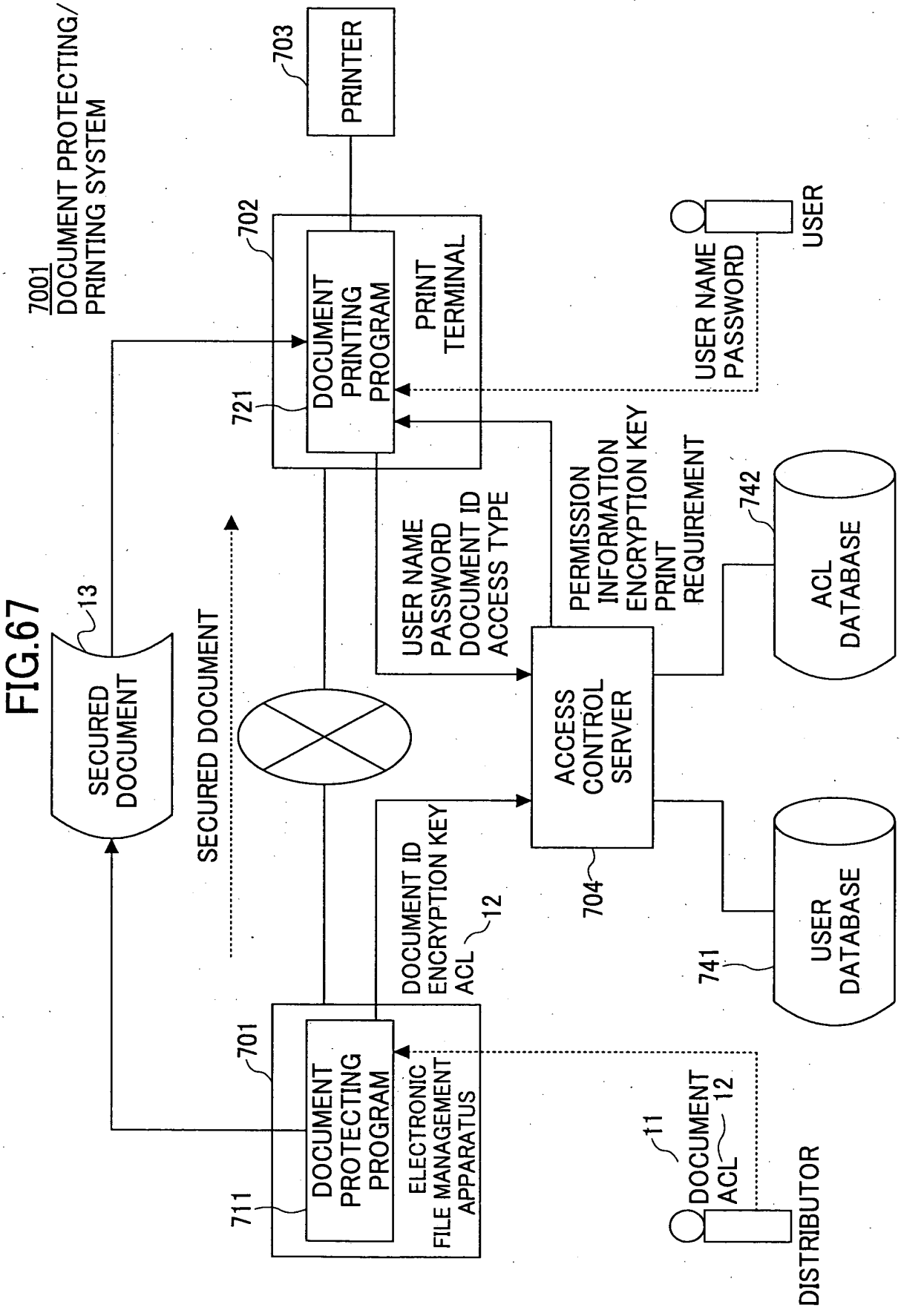
7001
DOCUMENT PROTECTING/
PRINTING SYSTEM
703
PRINTER
702
DOCUMENT
PRINTING
PROGRAM
PRINT
TERMINAL
721
USER NAME
PASSWORD
USER
13
SECURED
DOCUMENT
SECURED DOCUMENT
USER NAME
PASSWORD
DOCUMENT ID
ACCESS TYPE
PERMISSION
INFORMATION
ENCRYPTION KEY
PRINT
REQUIREMENT
742
ACL
DATABASE
ACCESS
CONTROL
SERVER
704
DOCUMENT ID
ENCRYPTION KEY
ACL
12
741
USER
DATABASE
701
DOCUMENT
PROTECTING
PROGRAM
ELECTRONIC
FILE MANAGEMENT
APPARATUS
711
11
DOCUMENT
ACL
12
DISTRIBUTOR

FIG.68

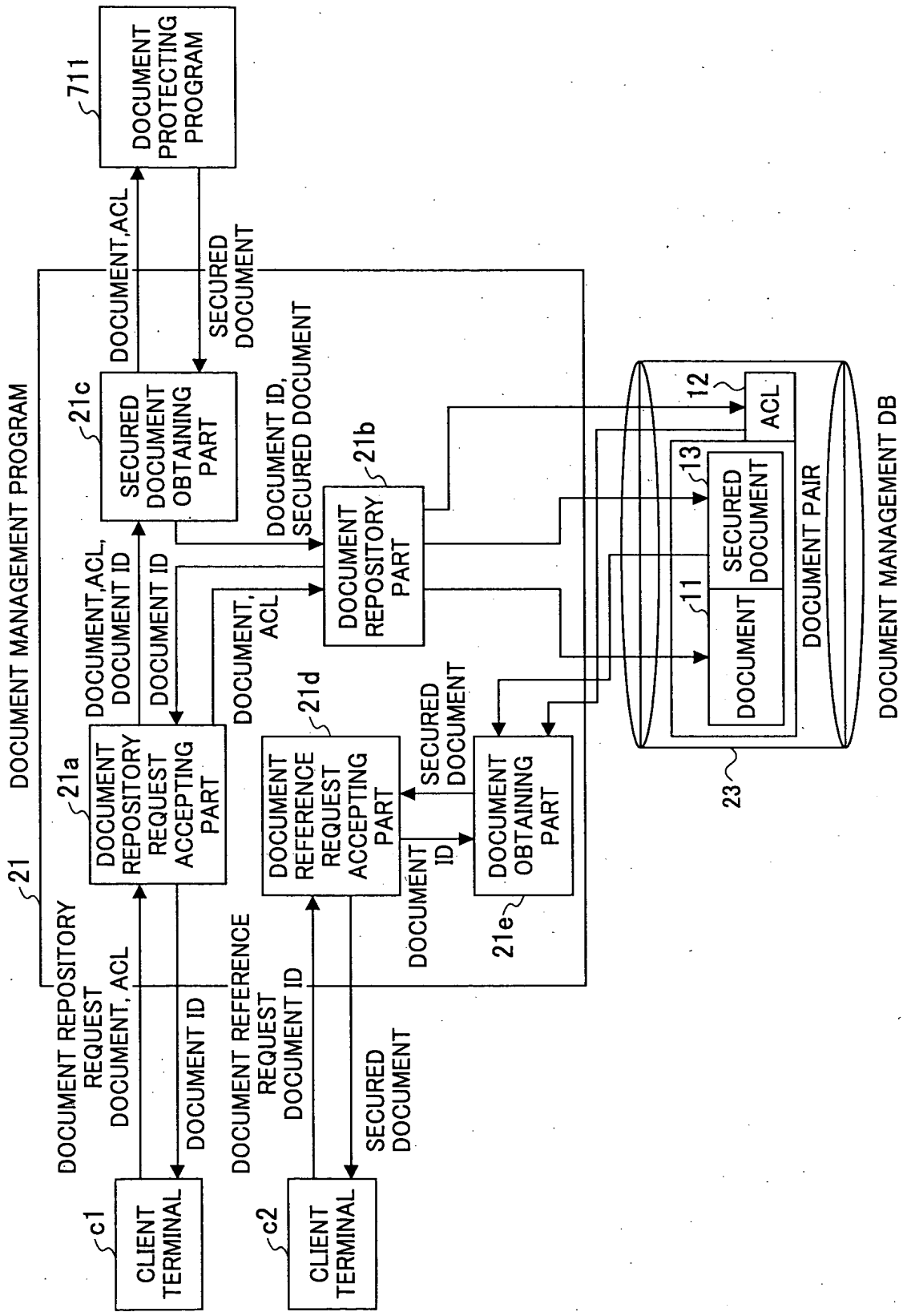
711
DOCUMENT PROTECTING PROGRAM
DOCUMENT,ACL
SECURED DOCUMENT
21
DOCUMENT MANAGEMENT PROGRAM
21c
SECURED DOCUMENT OBTAINING PART
DOCUMENT ID, SECURED DOCUMENT
21b
DOCUMENT REPOSITORY PART
12
ACL
13
SECURED DOCUMENT
11
DOCUMENT
DOCUMENT PAIR
DOCUMENT MANAGEMENT DB
23
DOCUMENT,ACL, DOCUMENT ID
DOCUMENT ID
DOCUMENT, ACL
21a
DOCUMENT REPOSITORY REQUEST ACCEPTING PART
21d
DOCUMENT REFERENCE REQUEST ACCEPTING PART
SECURED DOCUMENT
DOCUMENT ID
21e
DOCUMENT OBTAINING PART
DOCUMENT REPOSITORY REQUEST DOCUMENT, ACL
DOCUMENT ID
DOCUMENT REFERENCE REQUEST DOCUMENT ID
SECURED DOCUMENT
c1
CLIENT TERMINAL
c2
CLIENT TERMINAL

FIG.69

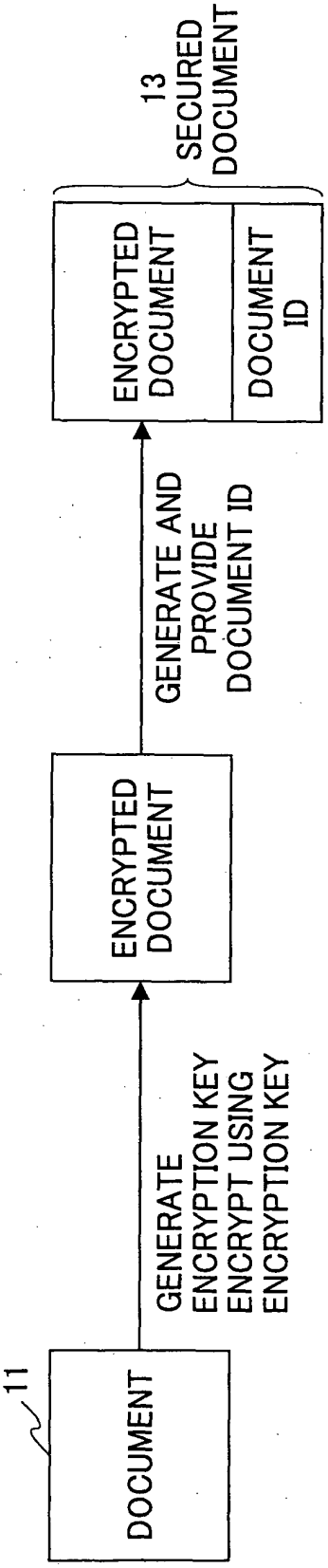
11
DOCUMENT
GENERATE ENCRYPTION KEY
ENCRYPT USING ENCRYPTION KEY
ENCRYPTED DOCUMENT
GENERATE AND PROVIDE DOCUMENT ID
13
SECURED DOCUMENT
ENCRYPTED DOCUMENT
DOCUMENT ID

FIG.70

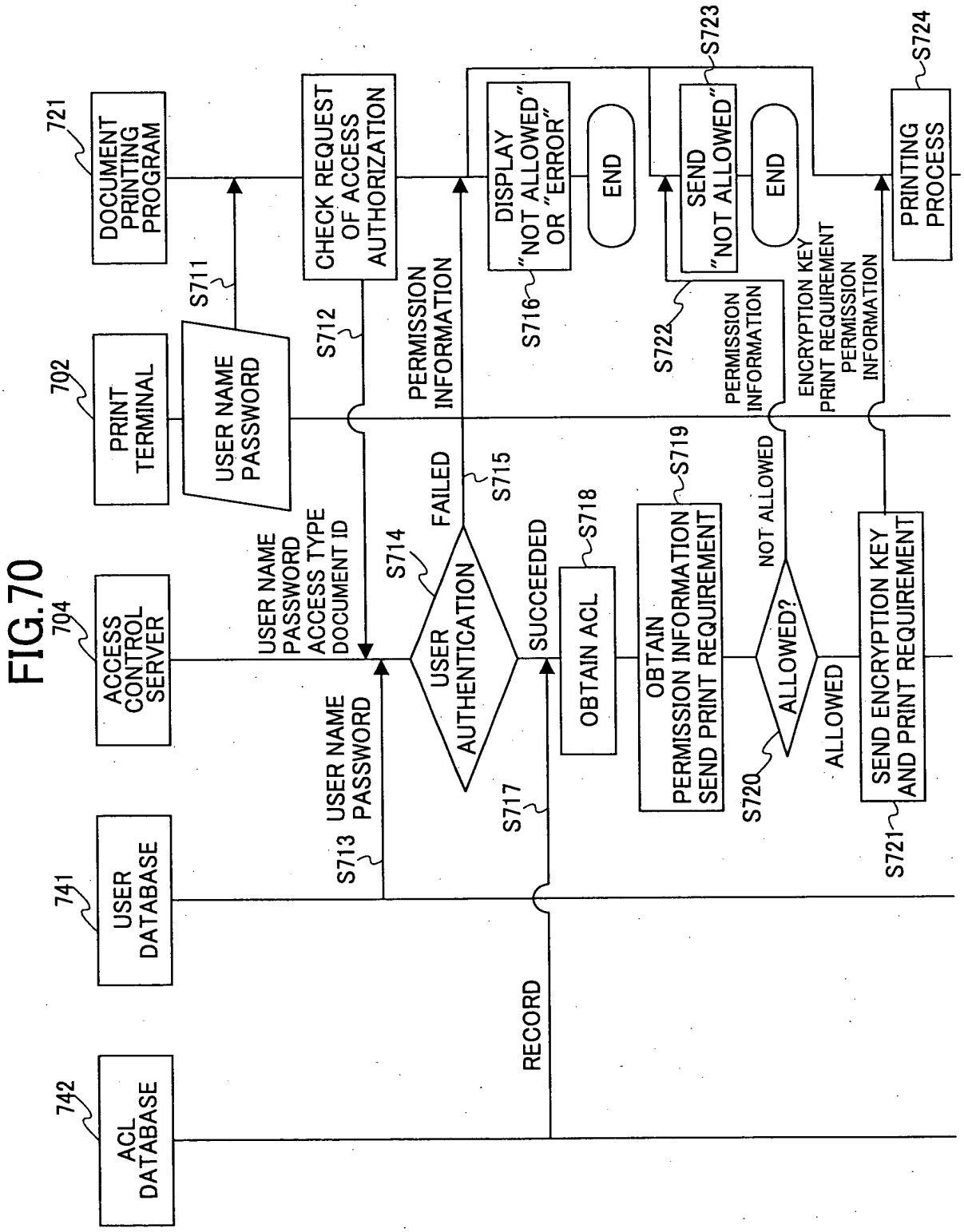
721
DOCUMENT PRINTING PROGRAM
702
PRINT TERMINAL
704
ACCESS CONTROL SERVER
741
USER DATABASE
742
ACL DATABASE
S711
USER NAME PASSWORD
S712
CHECK REQUEST OF ACCESS AUTHORIZATION
PERMISSION INFORMATION
S716
DISPLAY "NOT ALLOWED" OR "ERROR"
END
S722
S723
SEND "NOT ALLOWED"
END
S724
PRINTING PROCESS
USER NAME PASSWORD ACCESS TYPE DOCUMENT ID
S713
USER NAME PASSWORD
S714
USER AUTHENTICATION
FAILED
S715
SUCCEEDED
S717
RECORD
S718
OBTAIN ACL
S719
OBTAIN PERMISSION INFORMATION SEND PRINT REQUIREMENT
S720
ALLOWED?
NOT ALLOWED
PERMISSION INFORMATION
ENCRYPTION KEY PRINT REQUIREMENT PERMISSION INFORMATION
ALLOWED
S721
SEND ENCRYPTION KEY AND PRINT REQUIREMENT

FIG.71A

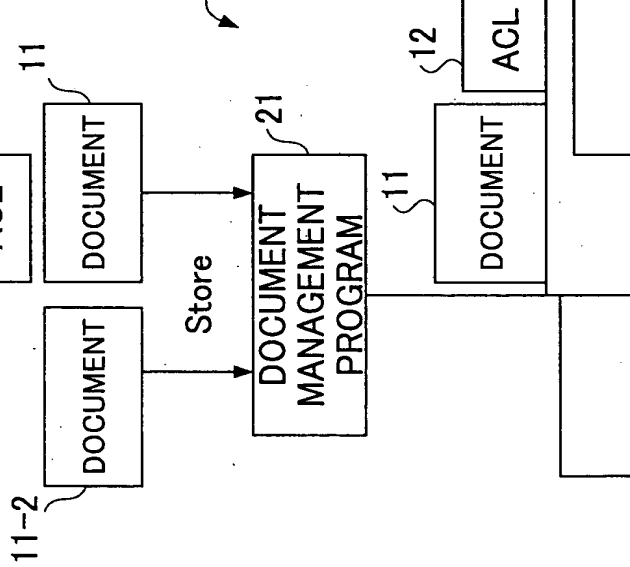

FIG.71B

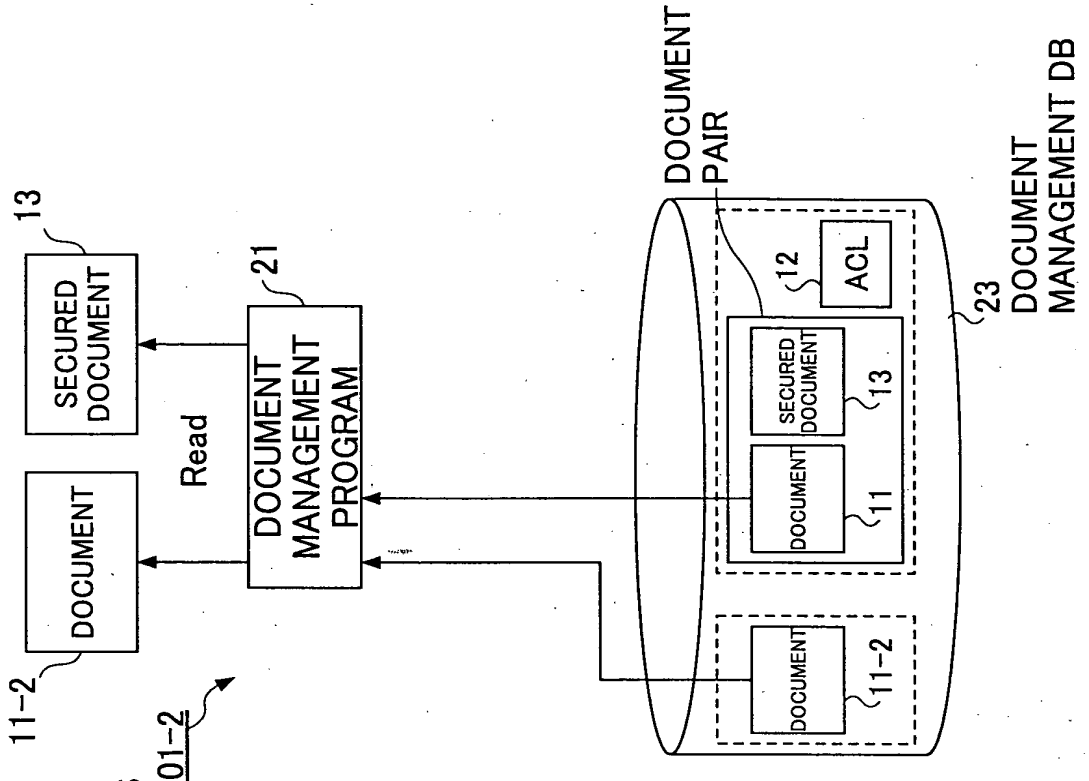

FIG.72A

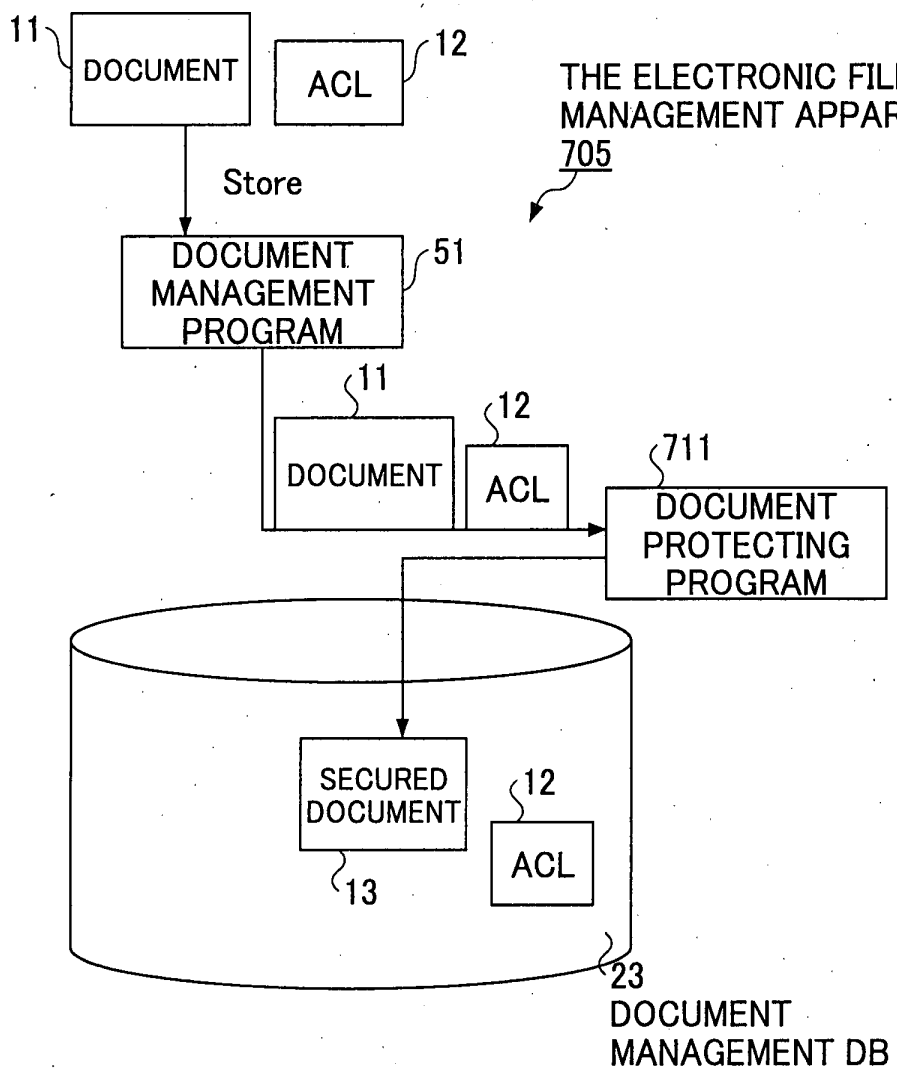

FIG.72B

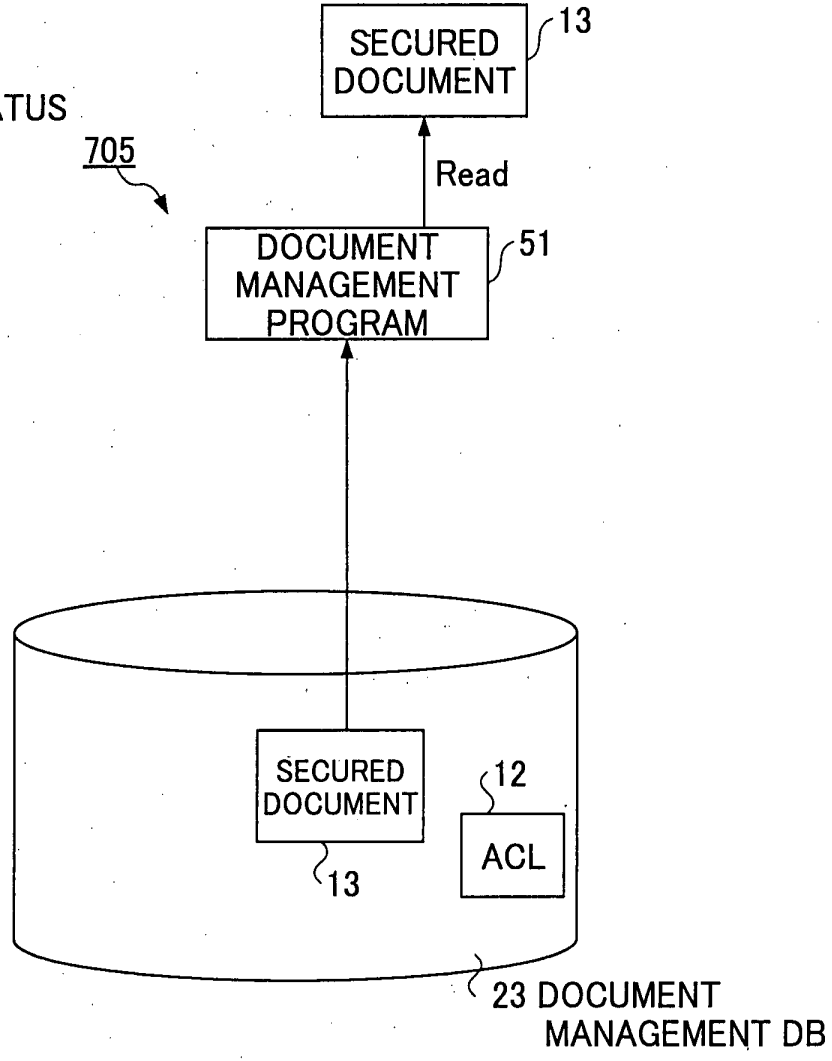

FIG.73A

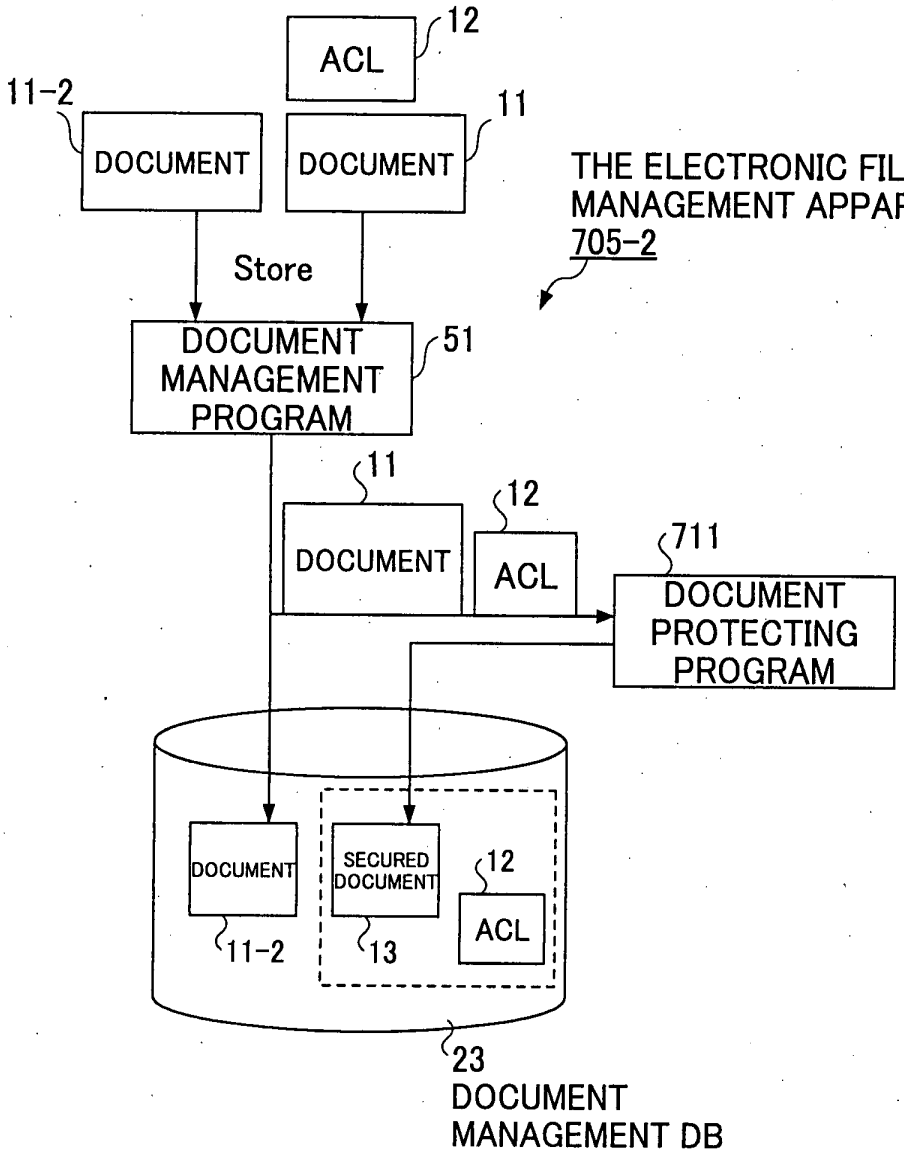

FIG.73B

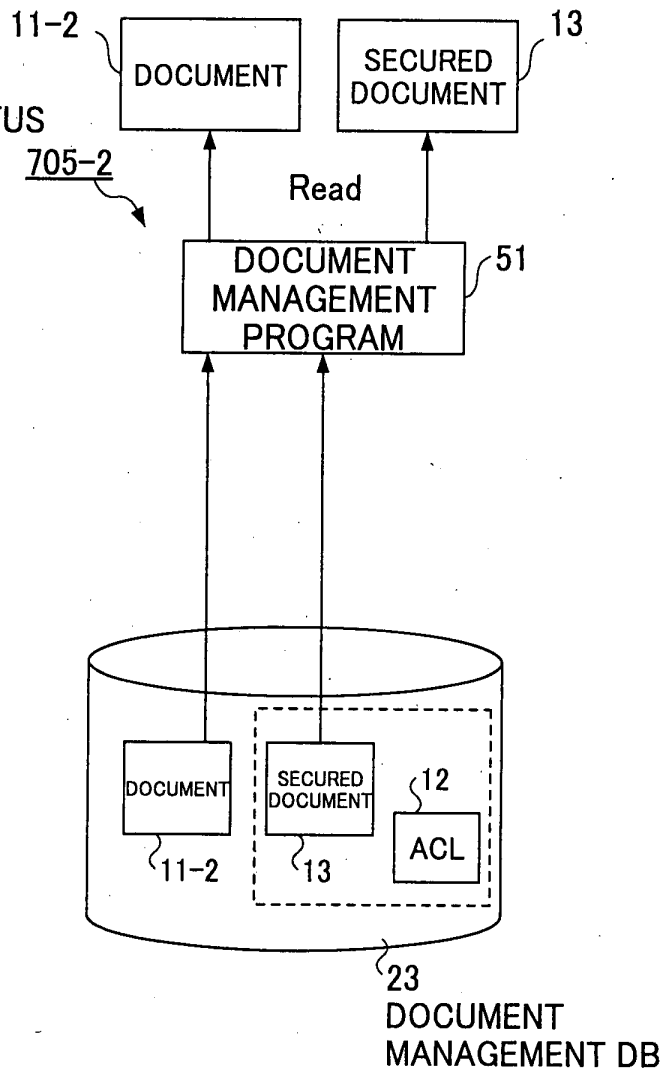

FIG.74

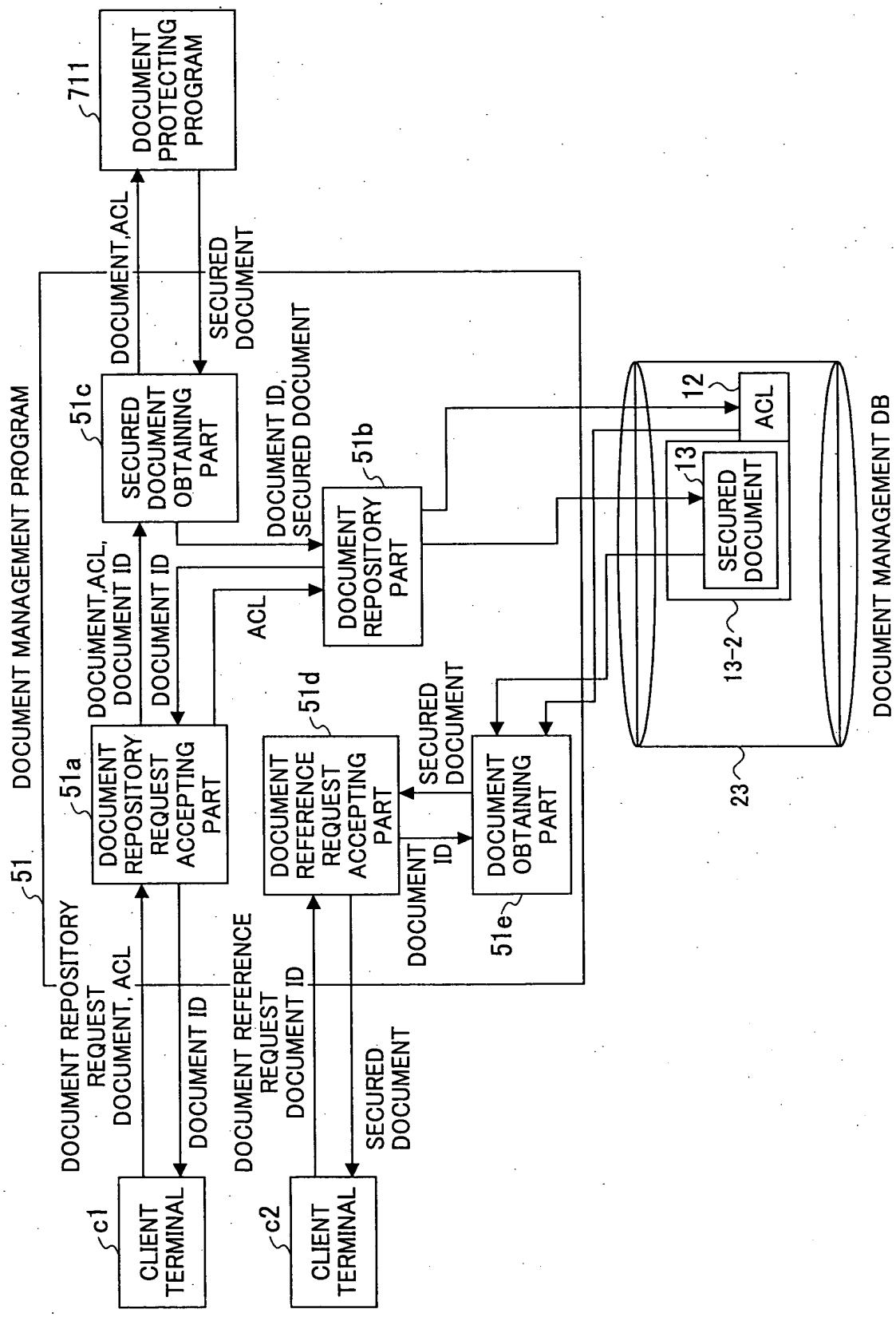
DOCUMENT MANAGEMENT PROGRAM
51
711
DOCUMENT PROTECTING PROGRAM
DOCUMENT,ACL
SECURED DOCUMENT
51c
SECURED DOCUMENT OBTAINING PART
DOCUMENT ID, SECURED DOCUMENT
51b
DOCUMENT REPOSITORY PART
12
ACL
13
SECURED DOCUMENT
13-2
23
DOCUMENT MANAGEMENT DB
DOCUMENT,ACL, DOCUMENT ID
DOCUMENT ID
ACL
51a
DOCUMENT REPOSITORY REQUEST ACCEPTING PART
51d
DOCUMENT REFERENCE REQUEST ACCEPTING PART
SECURED DOCUMENT
DOCUMENT ID
51e
DOCUMENT OBTAINING PART
DOCUMENT REPOSITORY REQUEST DOCUMENT, ACL
DOCUMENT ID
DOCUMENT REFERENCE REQUEST DOCUMENT ID
SECURED DOCUMENT
c1
CLIENT TERMINAL
c2
CLIENT TERMINAL

FIG.75A

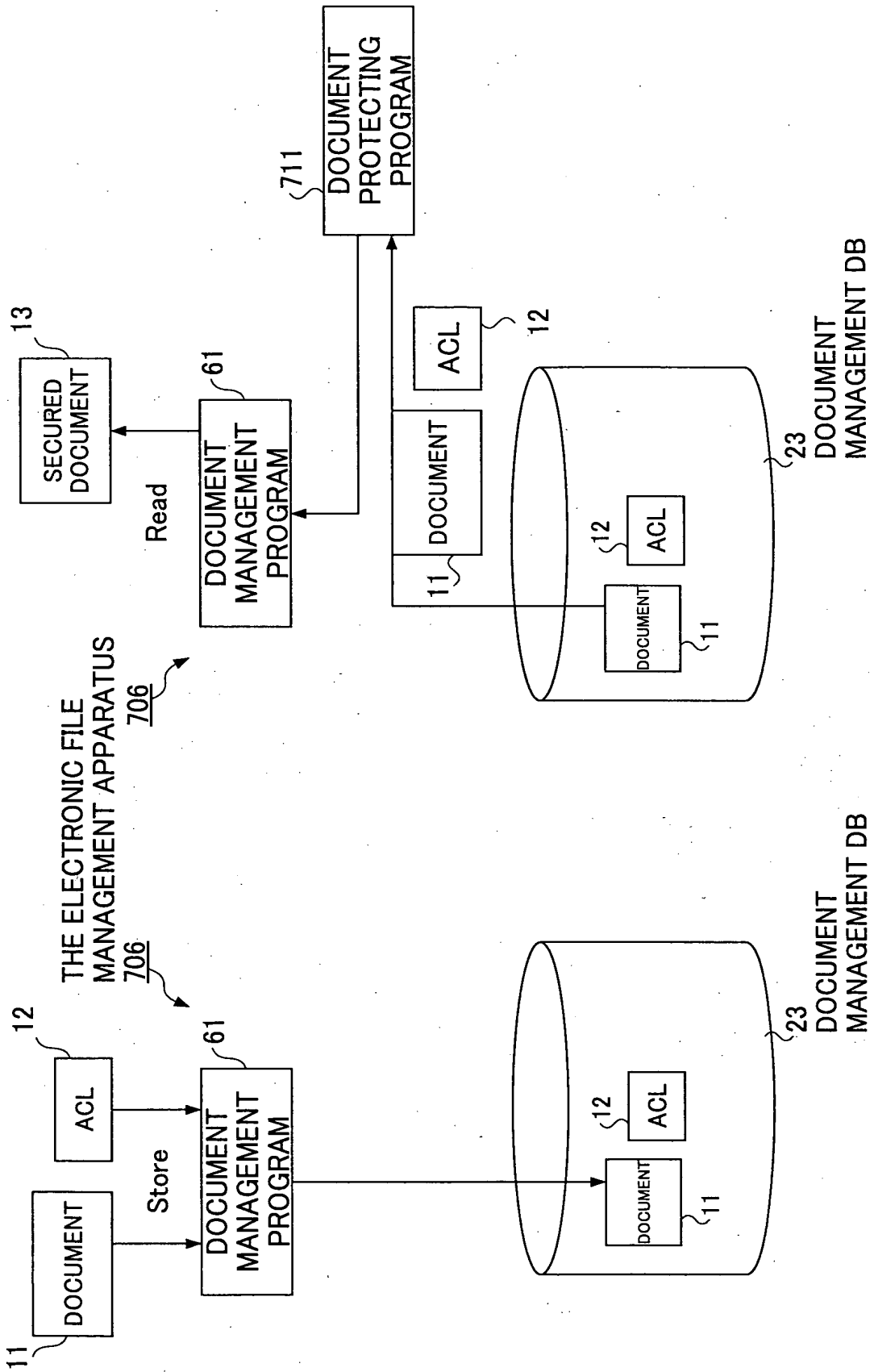

FIG.75B

FIG.76A

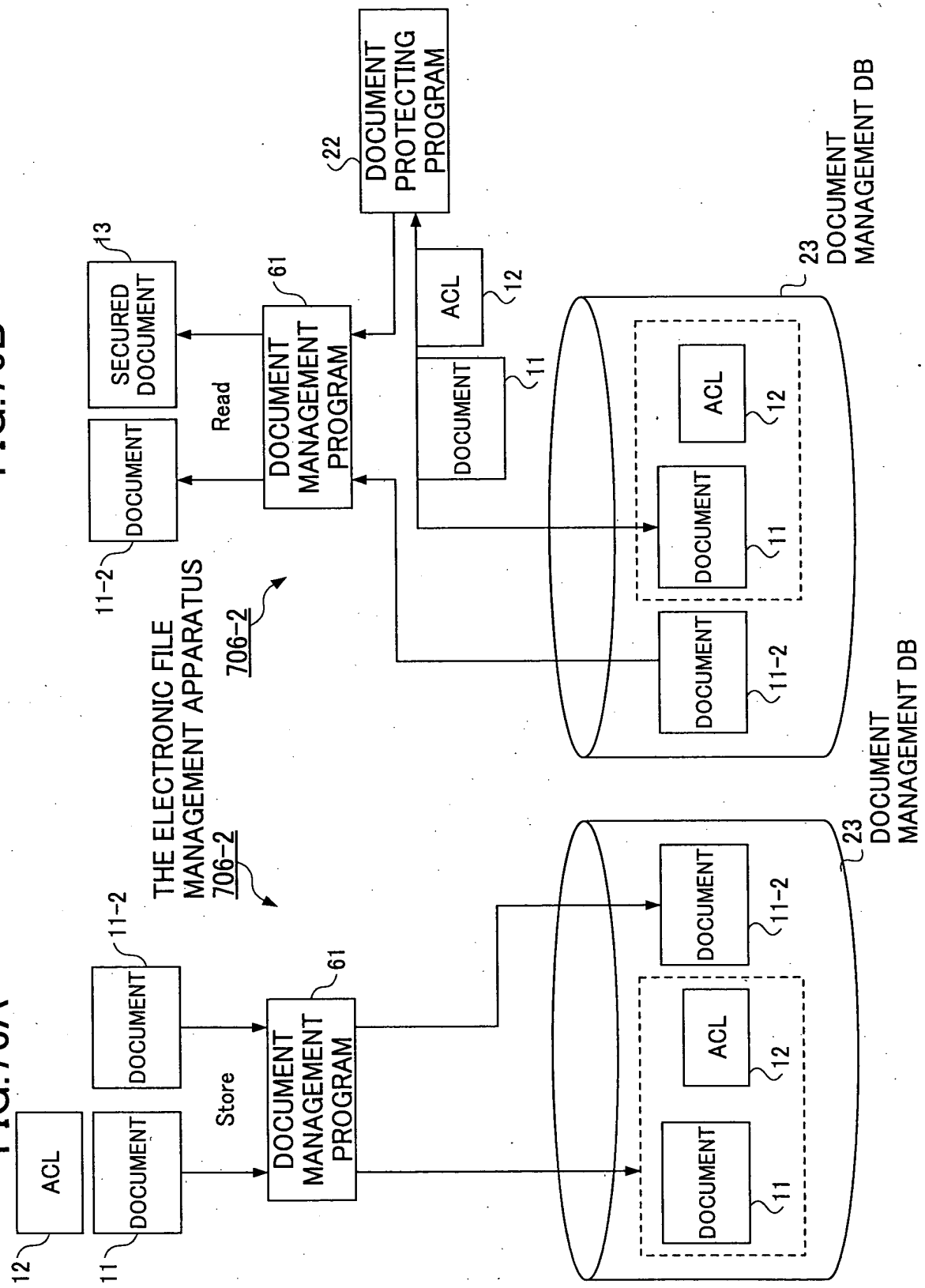

FIG.76B

FIG.77

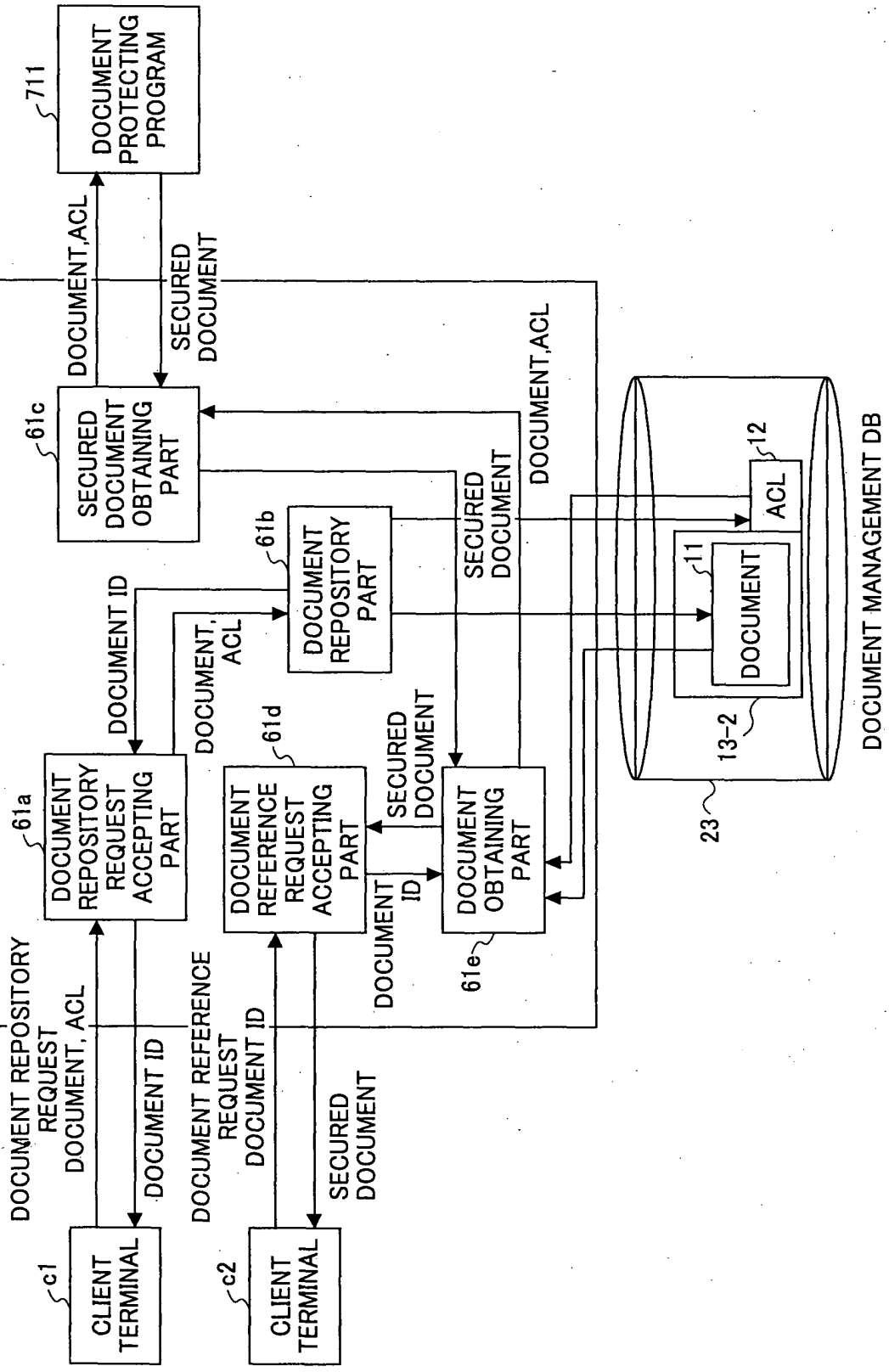
DOCUMENT MANAGEMENT PROGRAM
61
711
DOCUMENT PROTECTING PROGRAM
DOCUMENT,ACL
SECURED DOCUMENT
61c
SECURED DOCUMENT OBTAINING PART
61b
DOCUMENT REPOSITORY PART
61a
DOCUMENT REPOSITORY REQUEST ACCEPTING PART
61d
DOCUMENT REFERENCE REQUEST ACCEPTING PART
61e
DOCUMENT OBTAINING PART
DOCUMENT ID
DOCUMENT, ACL
SECURED DOCUMENT
DOCUMENT REPOSITORY REQUEST
DOCUMENT, ACL
DOCUMENT ID
DOCUMENT REFERENCE REQUEST
DOCUMENT ID
SECURED DOCUMENT
c1
CLIENT TERMINAL
c2
CLIENT TERMINAL
23
13-2
11
DOCUMENT
12
ACL
DOCUMENT MANAGEMENT DB

FIG.78A

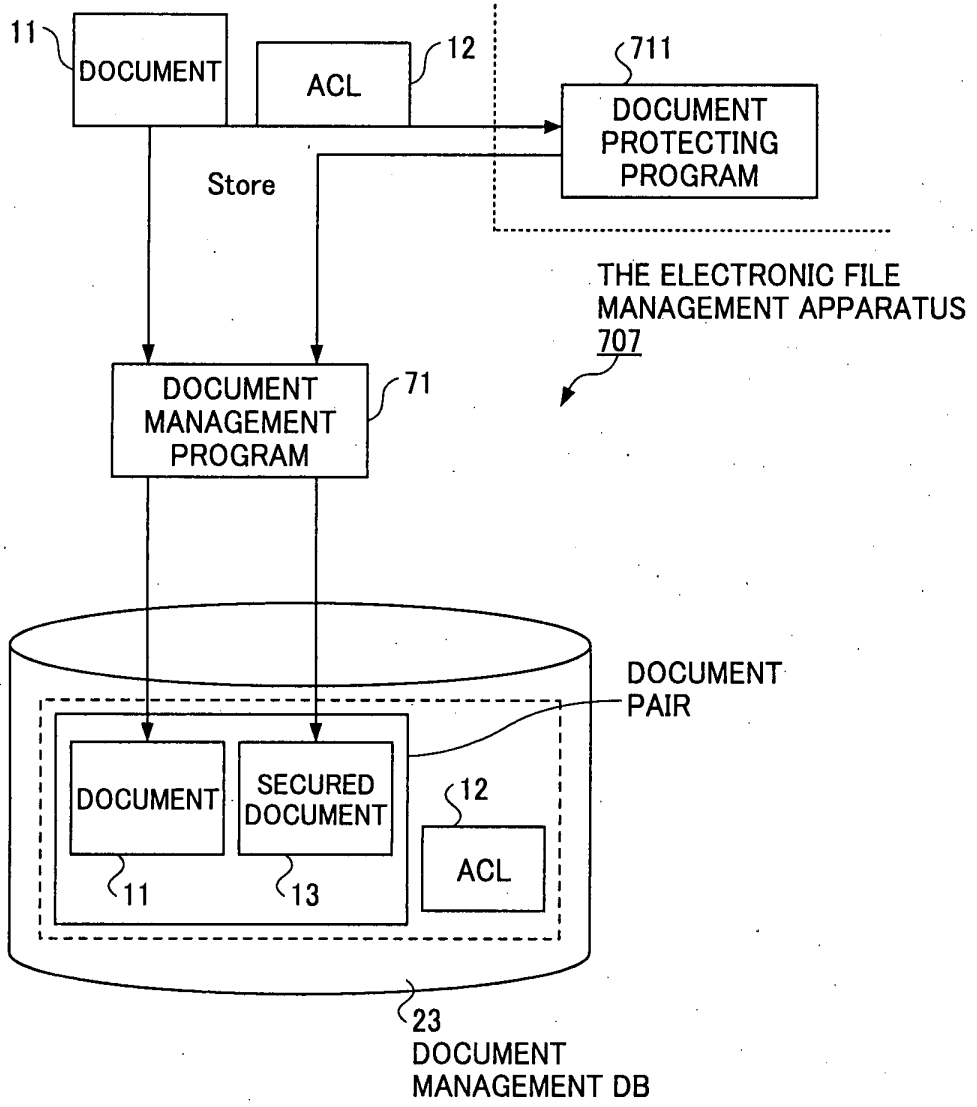

FIG.78B

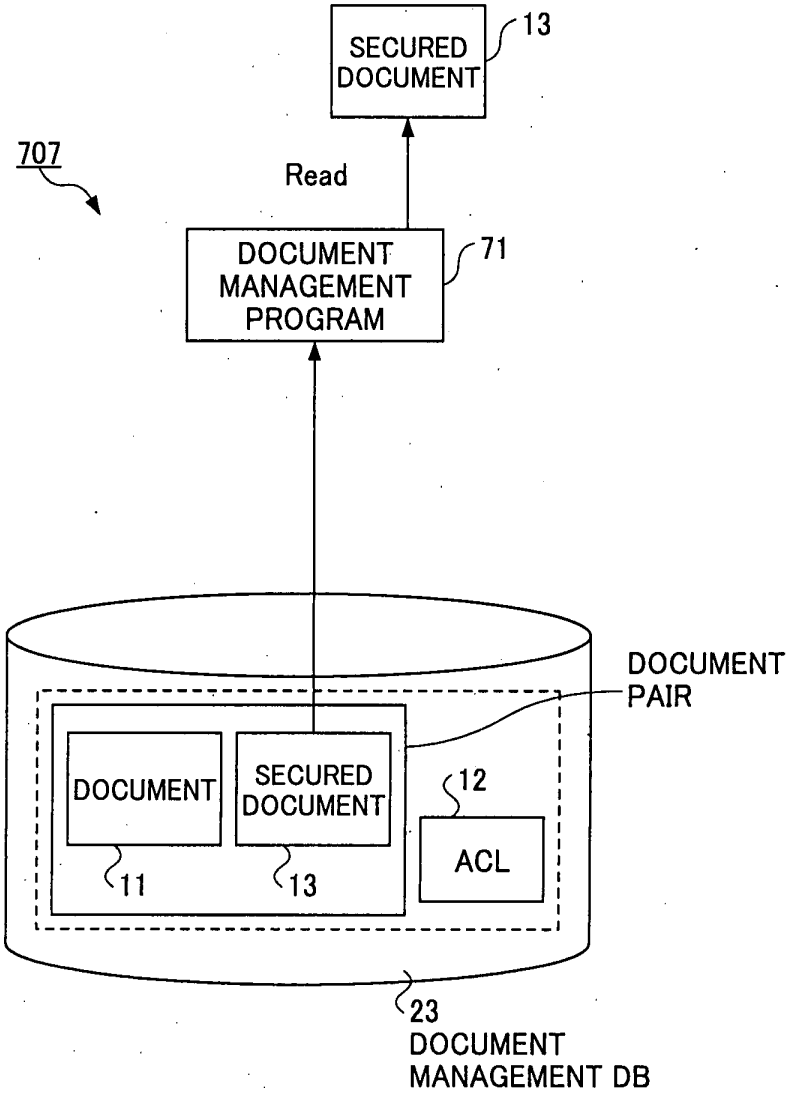

FIG.79A

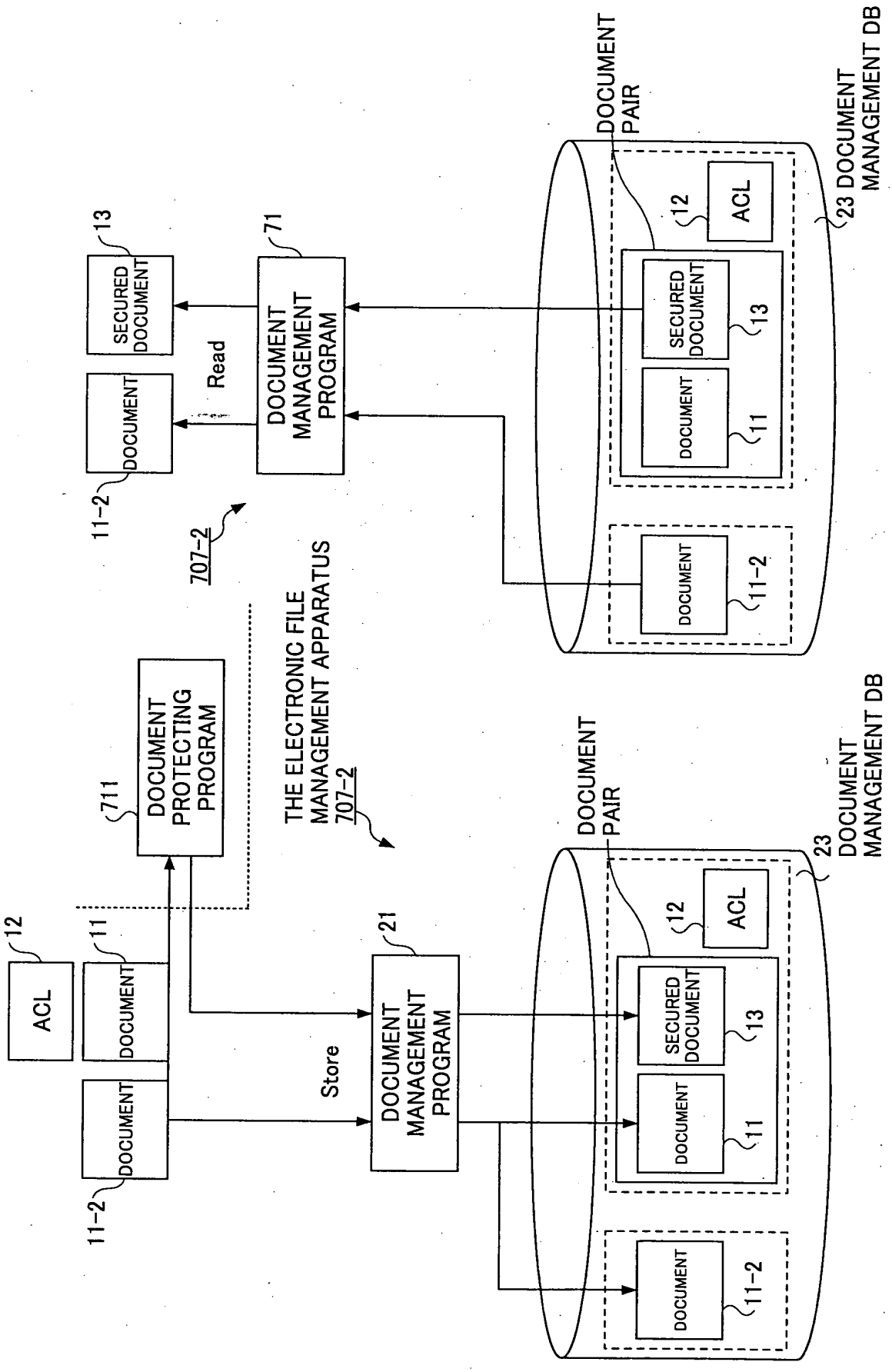

FIG.79B

FIG.80

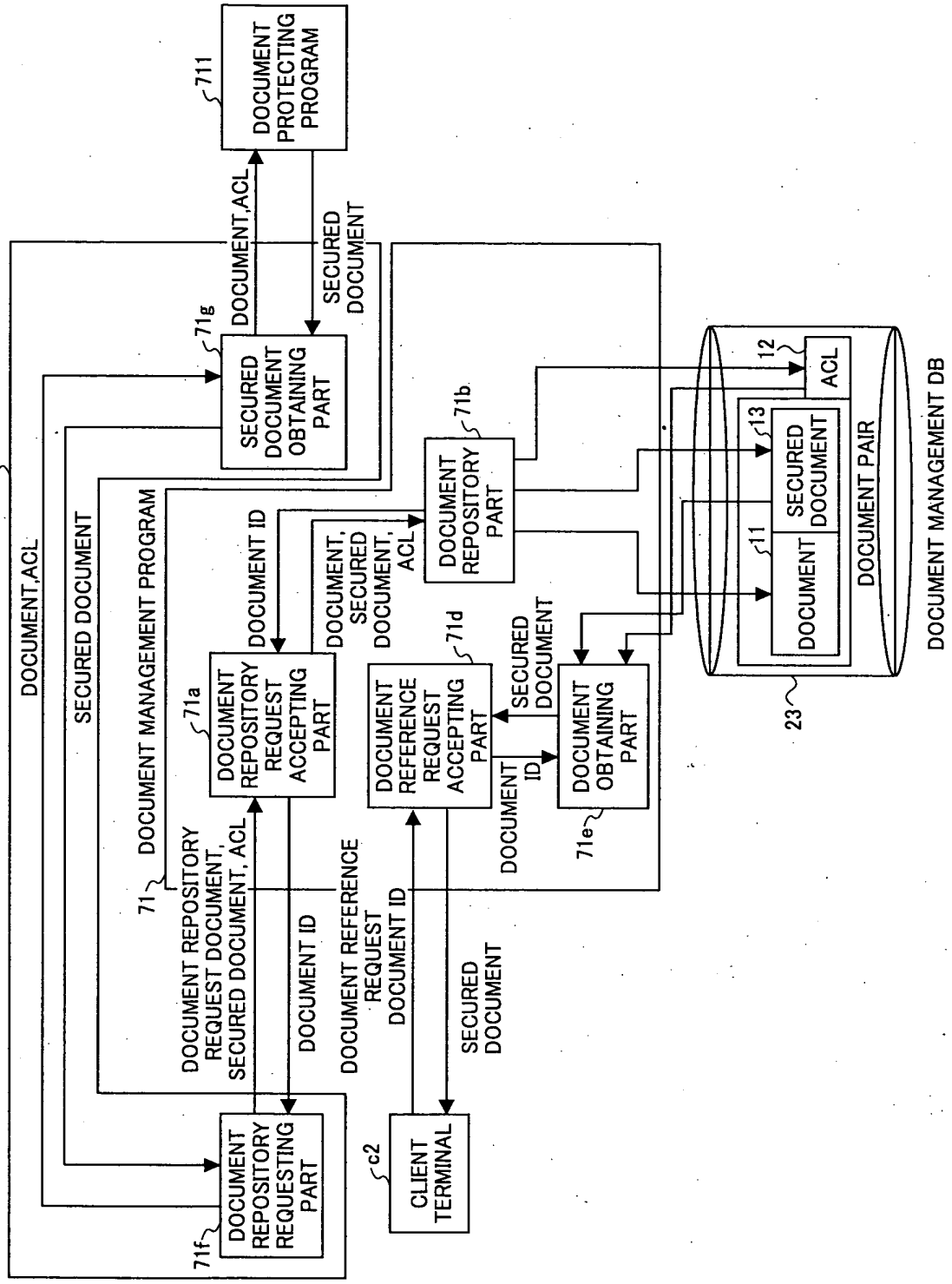
c1-2 CLIENT TERMINAL
DOCUMENT,ACL
SECURED DOCUMENT
DOCUMENT MANAGEMENT PROGRAM
71
DOCUMENT REPOSITORY REQUEST DOCUMENT, SECURED DOCUMENT, ACL
DOCUMENT ID
DOCUMENT REFERENCE REQUEST DOCUMENT ID
SECURED DOCUMENT
DOCUMENT ID
71f
DOCUMENT REPOSITORY REQUESTING PART
71a
DOCUMENT REPOSITORY REQUEST ACCEPTING PART
71d
DOCUMENT REFERENCE REQUEST ACCEPTING PART
71e
DOCUMENT OBTAINING PART
71g
SECURED DOCUMENT OBTAINING PART
711
DOCUMENT PROTECTING PROGRAM
DOCUMENT,ACL
SECURED DOCUMENT
DOCUMENT, SECURED DOCUMENT, ACL
71b
DOCUMENT REPOSITORY PART
c2
CLIENT TERMINAL
12
ACL
13
SECURED DOCUMENT
11
DOCUMENT
DOCUMENT PAIR
23
DOCUMENT MANAGEMENT DB

FIG.81

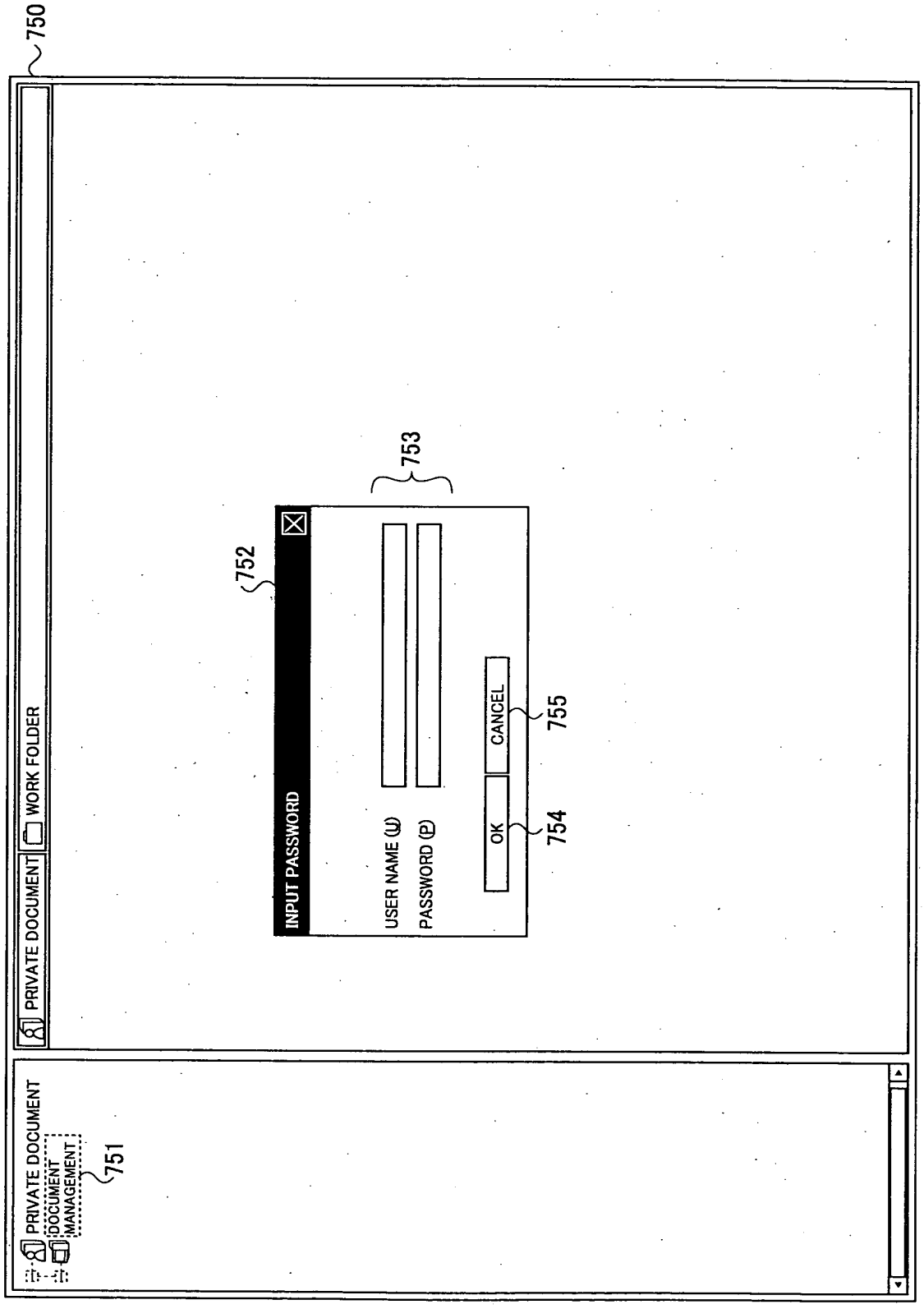
750
PRIVATE DOCUMENT
WORK FOLDER
PRIVATE DOCUMENT
DOCUMENT MANAGEMENT
751
752
753
INPUT PASSWORD
USER NAME (U)
PASSWORD (P)
OK
CANCEL
754
755

FIG.82

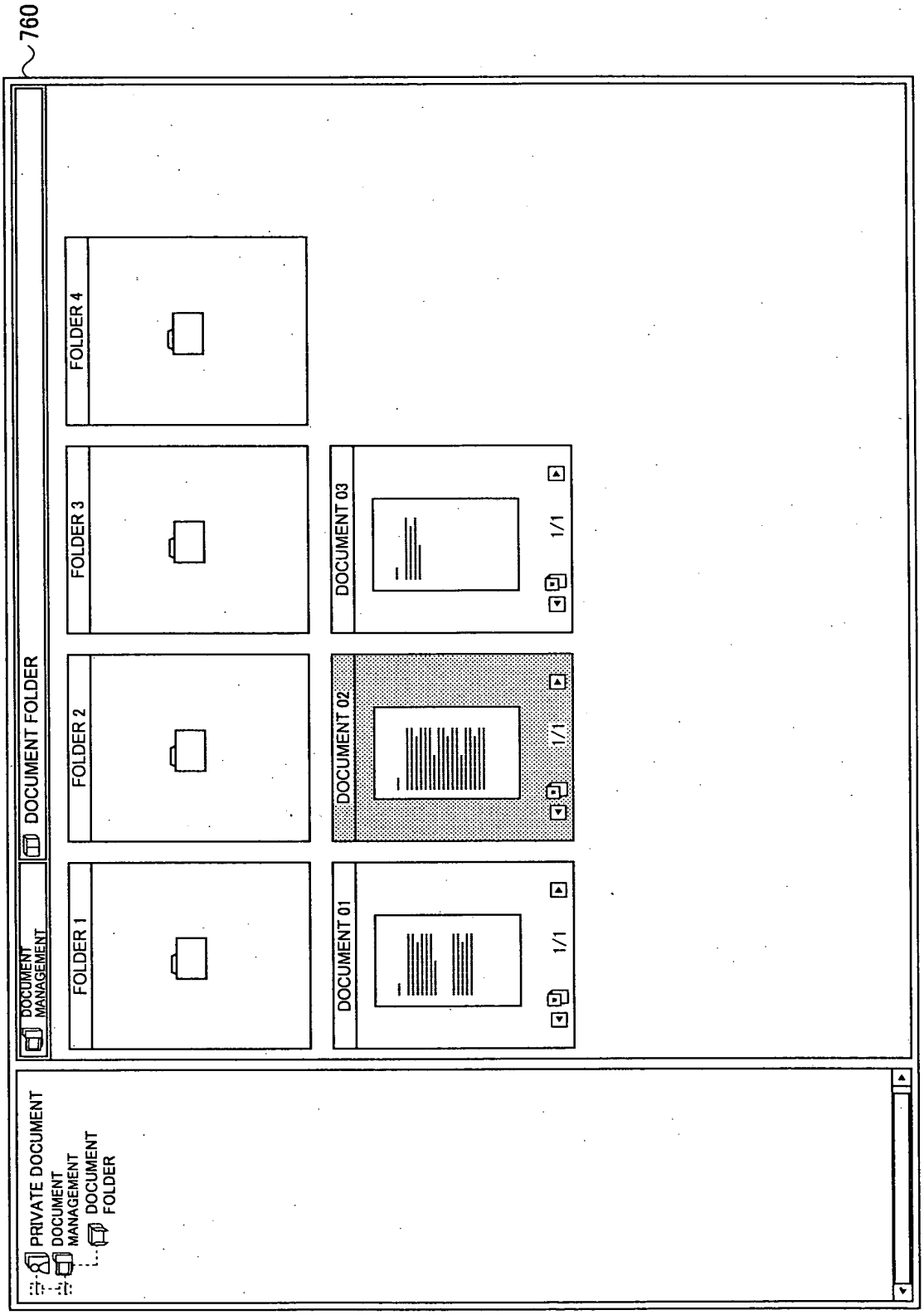
760
PRIVATE DOCUMENT
DOCUMENT MANAGEMENT
DOCUMENT FOLDER
DOCUMENT MANAGEMENT
DOCUMENT FOLDER
FOLDER 1
FOLDER 2
FOLDER 3
FOLDER 4
DOCUMENT 01
DOCUMENT 02
DOCUMENT 03
1/1
1/1
1/1

FIG.83

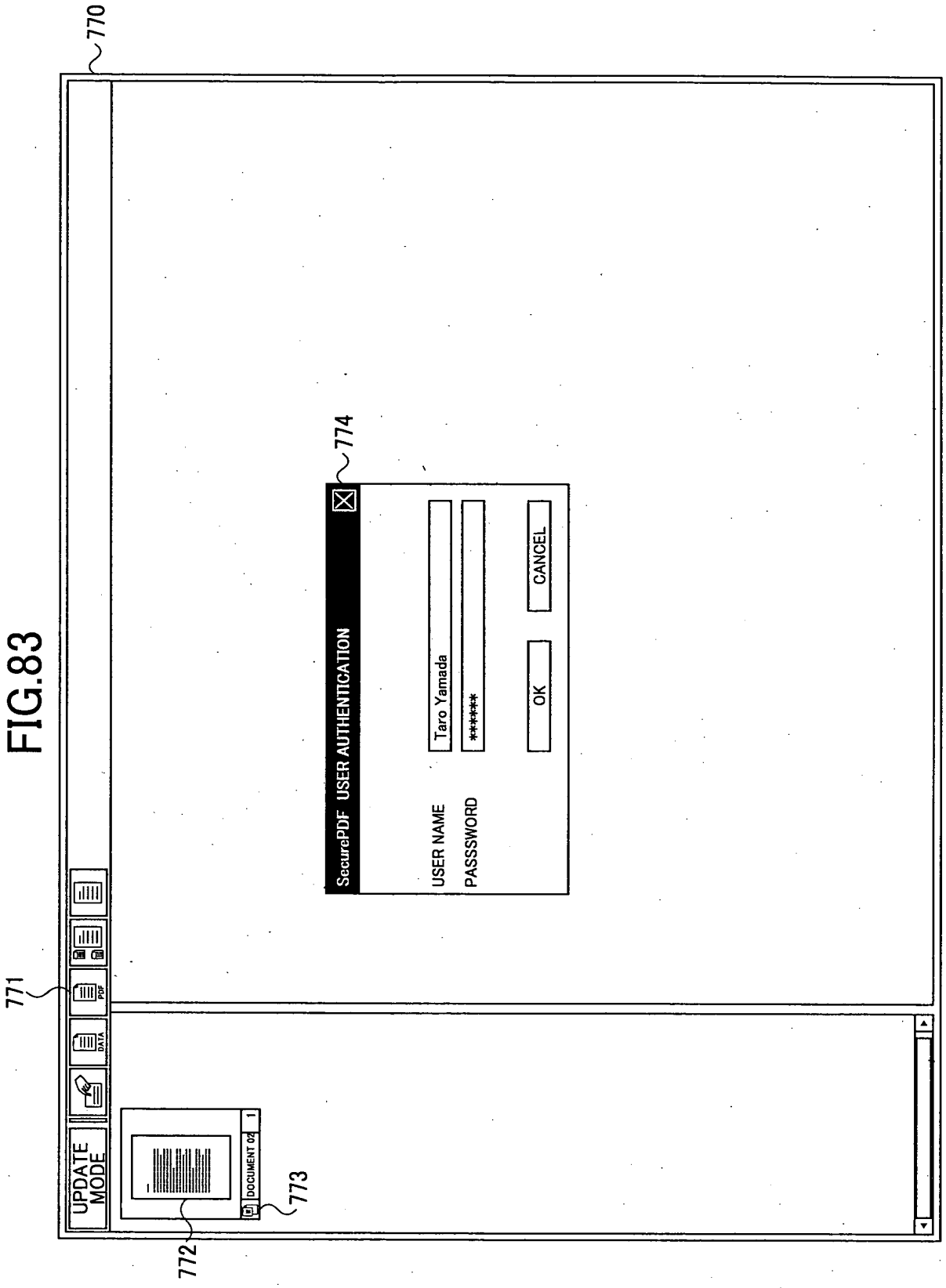
770
771
772
773
774
UPDATE MODE
DATA
PDF
DOCUMENT 02
SecurePDF USER AUTHENTICATION
USER NAME
PASSSWORD
Taro Yamada
******
OK
CANCEL

FIG.84

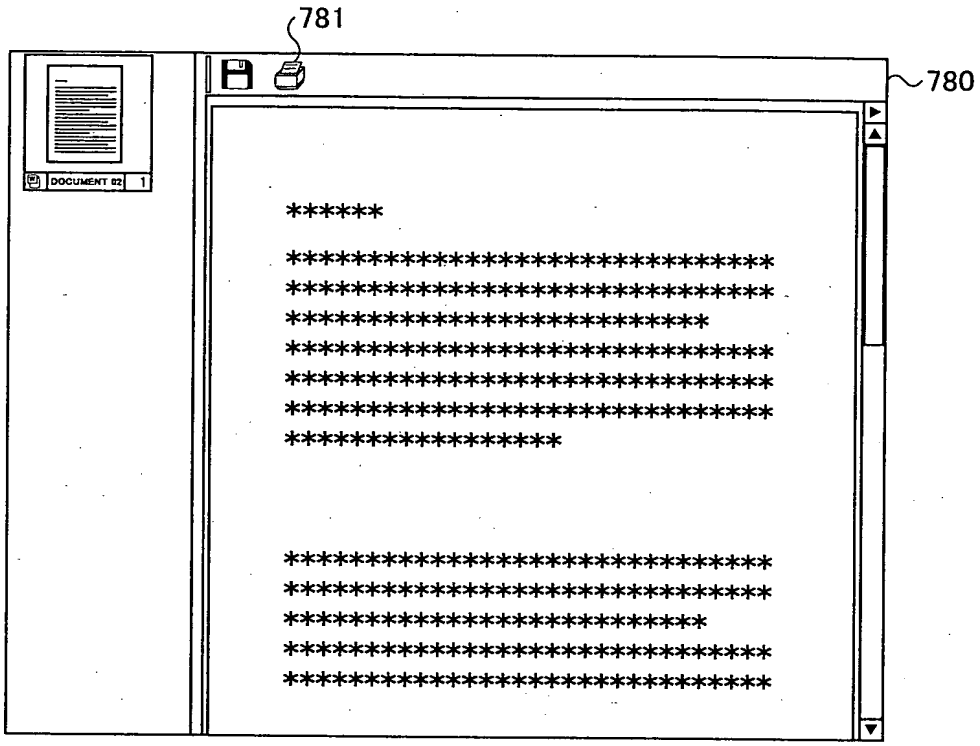

FIG.85

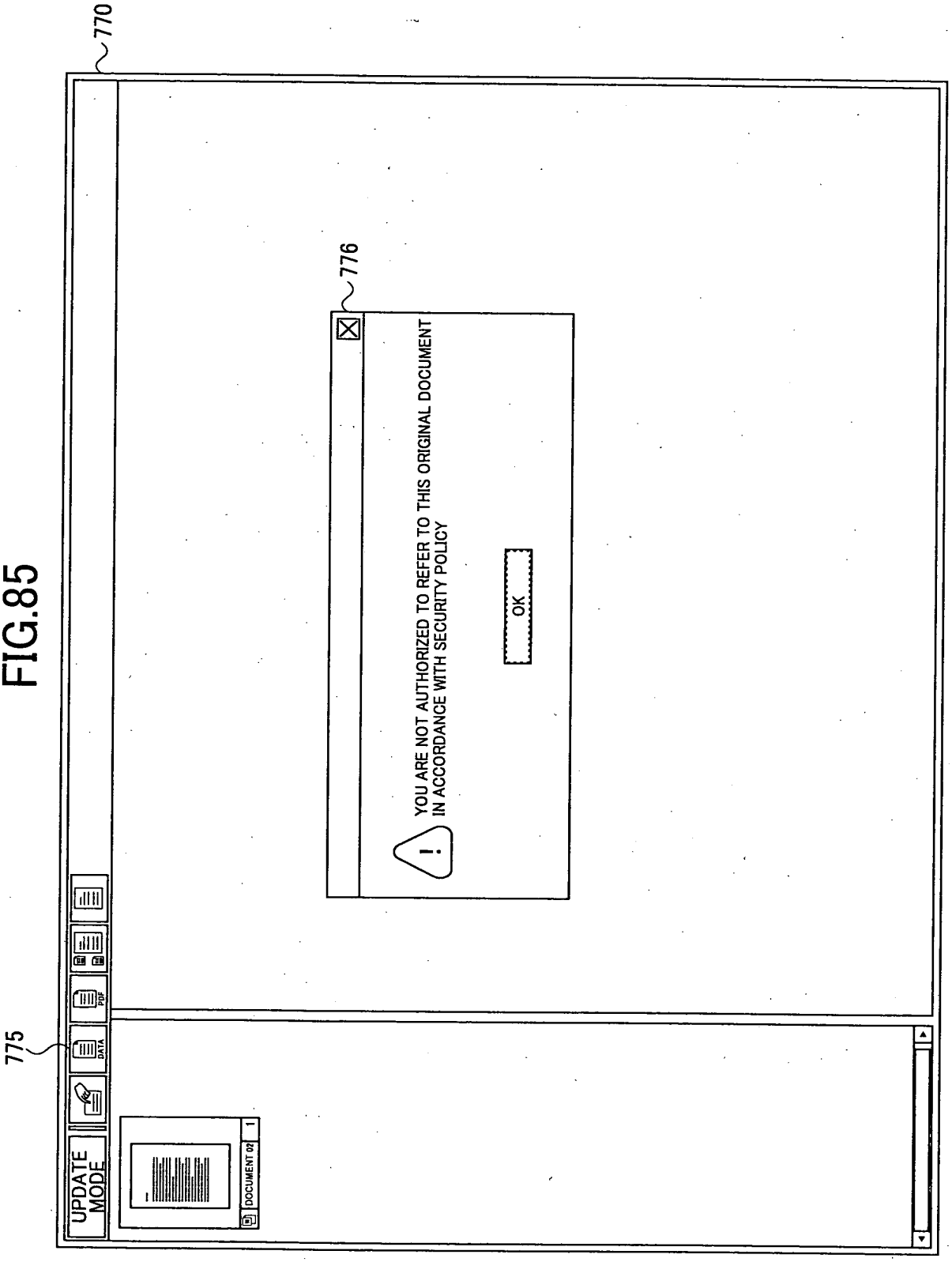
770
775
776
UPDATE MODE
DATA
PDF
DOCUMENT 02
YOU ARE NOT AUTHORIZED TO REFER TO THIS ORIGINAL DOCUMENT IN ACCORDANCE WITH SECURITY POLICY
OK

FIG.86

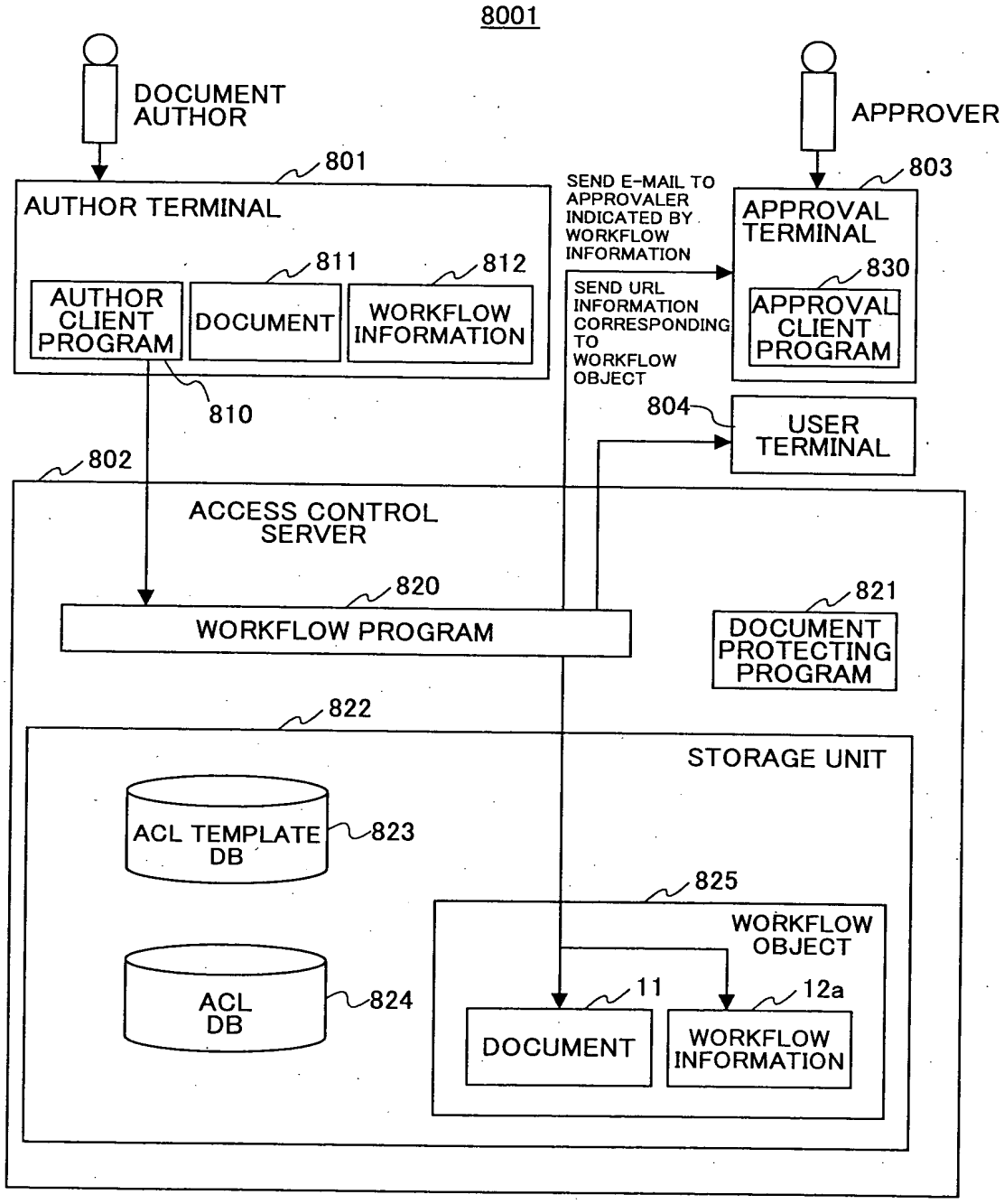
8001
DOCUMENT AUTHOR
APPROVER
801
AUTHOR TERMINAL
811
812
AUTHOR CLIENT PROGRAM
DOCUMENT
WORKFLOW INFORMATION
810
SEND E-MAIL TO APPROVALER INDICATED BY WORKFLOW INFORMATION
SEND URL INFORMATION CORRESPONDING TO WORKFLOW OBJECT
803
APPROVAL TERMINAL
830
APPROVAL CLIENT PROGRAM
804
USER TERMINAL
802
ACCESS CONTROL SERVER
820
WORKFLOW PROGRAM
821
DOCUMENT PROTECTING PROGRAM
822
STORAGE UNIT
ACL TEMPLATE DB
823
825
WORKFLOW OBJECT
ACL DB
824
11
12a
DOCUMENT
WORKFLOW INFORMATION

FIG.87

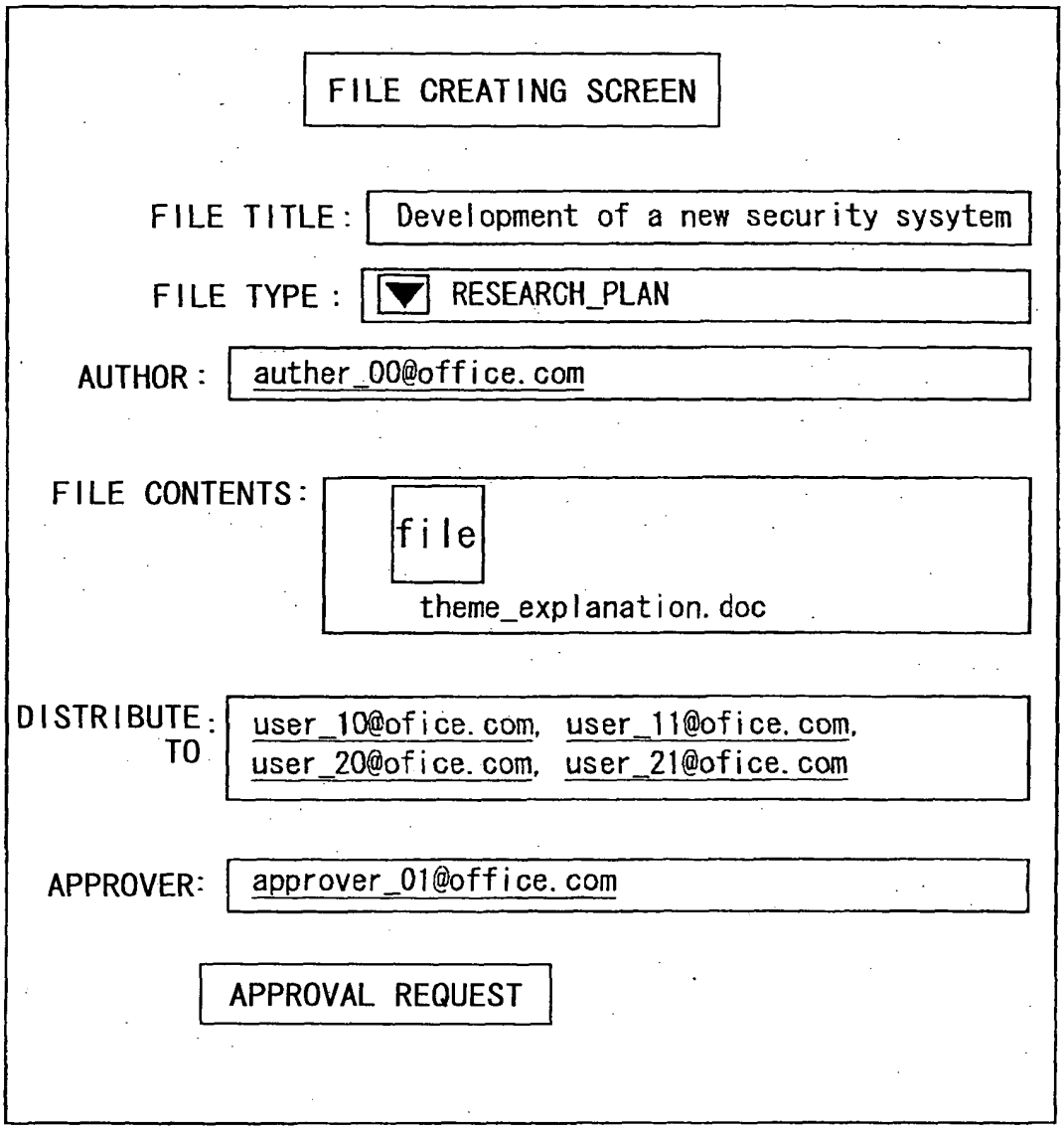
FILE CREATING SCREEN
FILE TITLE:
Development of a new security sysytem
FILE TYPE :
RESEARCH_PLAN
AUTHOR :
auther_00@office.com
FILE CONTENTS:
file
theme_explanation.doc
DISTRIBUTE TO:
user_10@ofice.com, user_11@ofice.com,
user_20@ofice.com, user_21@ofice.com
APPROVER:
approver_01@office.com
APPROVAL REQUEST

FIG.88

FILE NAME	Development of a new security system
FILE TYPE	RESEACH_PLAN
AUTHOR	author_00@office.com
APPROVAL	approver_01@office.com
FILE CONTENTS	theme_explanation.doc
DISTRIBUTE TO	user_10@office.com user_11@office.com user_20@office.com user_21@office.com

FIG.89

```
<?xml version="1.0"encording="UTF-8"?>
<workflow_info>
        <id>011237835</id>
        <title>Development of a new security sysytem</title>
        <doc_type>RESEARCH_PLAN</doc_type>
        <status>wait_for_approval</status>
        <author>author_00@office.com</author>
        <approver>approver_01@office.com</approver>
        <distribute_to>user_10@office.com</distribute_to>
        <distribute_to>user_10@office.com</distribute_to>
        <distribute_to>user_10@office.com</distribute_to>
        <distribute_to>user_10@office.com</distribute_to>
</workflow_info>
```

FIG.90

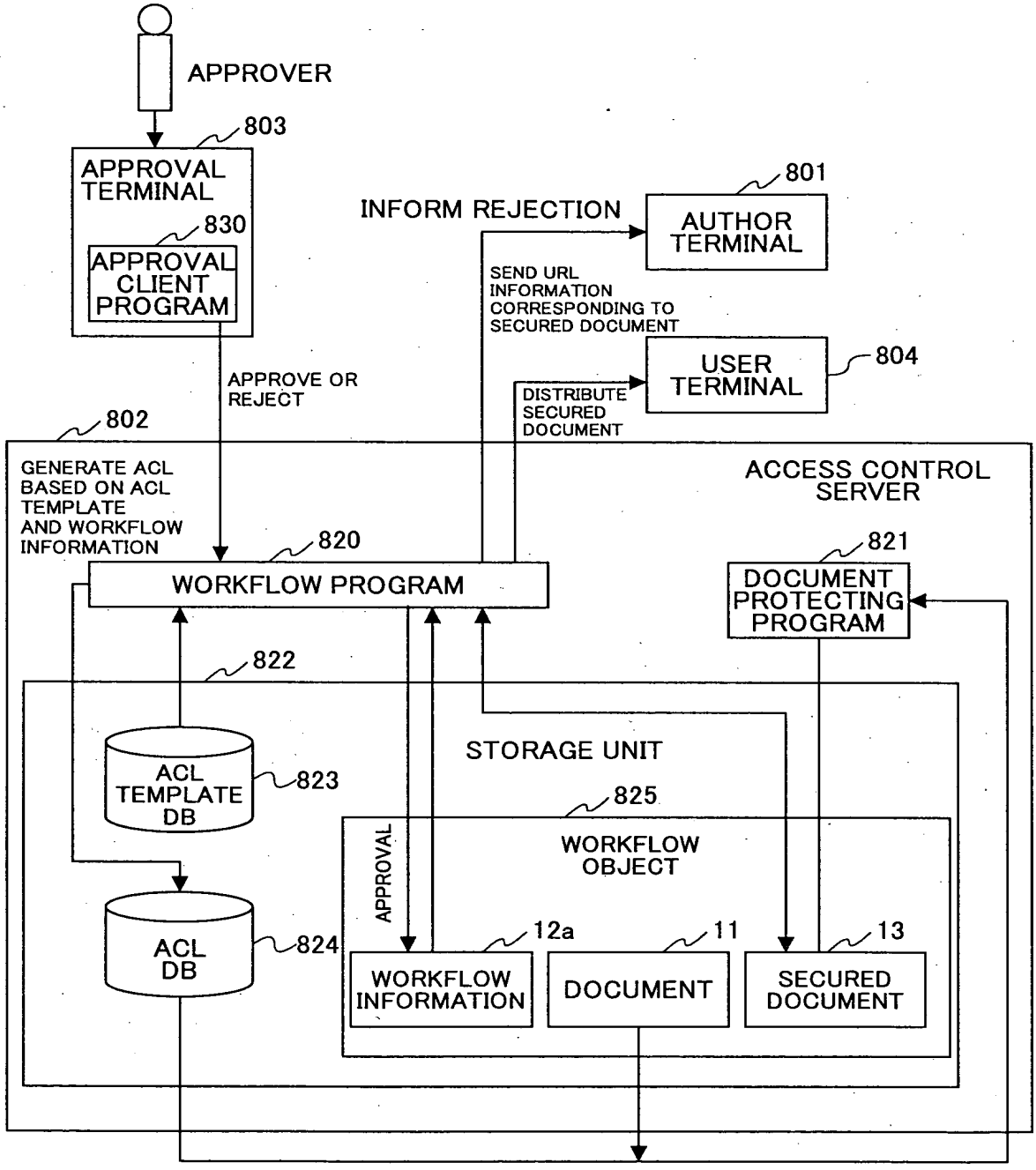
8002
APPROVER
803
APPROVAL TERMINAL
830
APPROVAL CLIENT PROGRAM
APPROVE OR REJECT
INFORM REJECTION
801
AUTHOR TERMINAL
SEND URL INFORMATION CORRESPONDING TO SECURED DOCUMENT
USER TERMINAL
804
DISTRIBUTE SECURED DOCUMENT
802
GENERATE ACL BASED ON ACL TEMPLATE AND WORKFLOW INFORMATION
ACCESS CONTROL SERVER
820
WORKFLOW PROGRAM
821
DOCUMENT PROTECTING PROGRAM
822
STORAGE UNIT
ACL TEMPLATE DB
823
825
WORKFLOW OBJECT
APPROVAL
ACL DB
824
12a
11
13
WORKFLOW INFORMATION
DOCUMENT
SECURED DOCUMENT

FIG.91

User type	Access type	Permission	Requirements
author	Read	Allowed	-
	Write	Denied	-
	Print	Allowed	PAC(Private Access)
	Hardcopy	Allowed	-
approver	Read	Allowed	-
	Write	Denied	-
	Print	Allowed	PAC(Private Access)
	Hardcopy	Allowed	-
distribute_to	Read	Allowed	-
	Write	Denied	-
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Pattern)
			EBC(Embedding Barcord)
	Hardcopy	Allowed	RAD(Record Audit Data)

FIG.92

User type	Access type	Permission	Requirements
author_00@office.com	Read	Allowed	-
	Write	Denied	-
	Print	Allowed	PAC(Private Access)
	Hardcopy	Allowed	-
approver_01@offide.com	Read	Allowed	-
	Write	Denied	-
	Print	Allowed	PAC(Private Access)
	Hardcopy	Allowed	-
user_10@office.com	Read	Allowed	-
	Write	Denied	-
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Pattern)
			EBC(Embedding Barcord)
	Hardcopy	Allowed	RAD(Record Audit Data)
user_11@office.com	Read	Allowed	-
	Write	Denied	-
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Pattern)
			EBC(Embedding Barcord)
	Hardcopy	Allowed	RAD(Record Audit Data)
user_20@office.com	Read	Allowed	-
	Write	Denied	-
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Pattern)
			EBC(Embedding Barcord)
	Hardcopy	Allowed	RAD(Record Audit Data)
user_21@office.com	Read	Allowed	-
	Write	Denied	-
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Pattern)
			EBC(Embedding Barcord)
	Hardcopy	Allowed	RAD(Record Audit Data)

FIG.93

Document type	Security attributes	
	Category	Sensitivity
RESEARCH_PLAN	Technical	Medium
GENERAL_CONTRACT	Contract	Basic
TOP_SECRET	General	High